

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-347850

(43)Date of publication of application : 15.12.2000

(51)Int.Cl. G06F 9/06  
G09C 1/00  
G10L 19/00  
H03M 7/00  
H04L 9/14

(21)Application number : 2000-087988

(22)Date of filing : 28.03.2000

(71)Applicant : SONY CORP

(72)Inventor : ISHIGURO RYUJI  
KAWAKAMI TATSU  
TANABE MITSURU  
EOMO YUICHI  
KAWAHARA HIROKAZU

(30)Priority

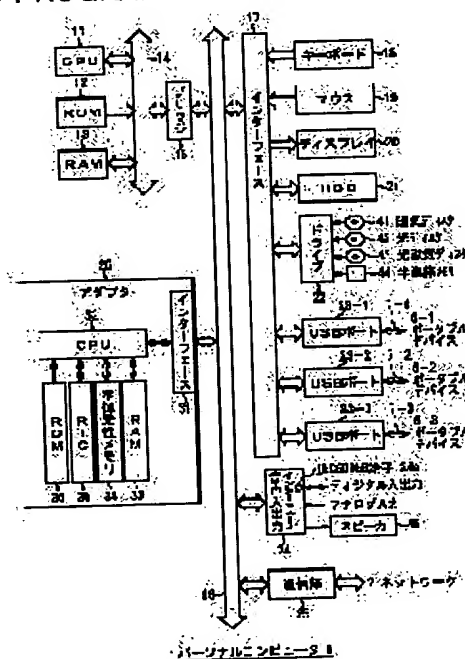
Priority number : 11088348 Priority date : 30.03.1999 Priority country : JP

## (54) DEVICE AND METHOD FOR INFORMATION PROCESSING AND PROGRAM STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent stored data from illegally being read out and analyzed.

SOLUTION: A CPU 11 rearranges instruction lines included in a program to be executed by an adapter 26. The CPU 11 ciphers the program. On an HDD(Hard Disk Drive) 21, the ciphered program having the instruction lines rearranged is recorded. An interface 17 transmits the program recorded on the HDD 21 to the adapter 26.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application]

converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-347850

(P 2 0 0 0 - 3 4 7 8 5 0 A)

(43) 公開日 平成12年12月15日 (2000. 12. 15)

(51) Int. Cl. <sup>7</sup>	識別記号	F I	テーマコード <sup>*</sup> (参考)
G06F 9/06	550	G06F 9/06	550 B
G09C 1/00	660	G09C 1/00	660 D
G10L 19/00		H03M 7/00	
H03M 7/00		G10L 9/00	N
H04L 9/14		H04L 9/00	641
審査請求 未請求 請求項の数 5 O L (全48頁)			

(21) 出願番号 特願2000-87988 (P 2000-87988)

(22) 出願日 平成12年3月28日 (2000. 3. 28)

(31) 優先権主張番号 特願平11-88348

(32) 優先日 平成11年3月30日 (1999. 3. 30)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 石黒 隆二

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 河上 達

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100082131

弁理士 稲本 義雄

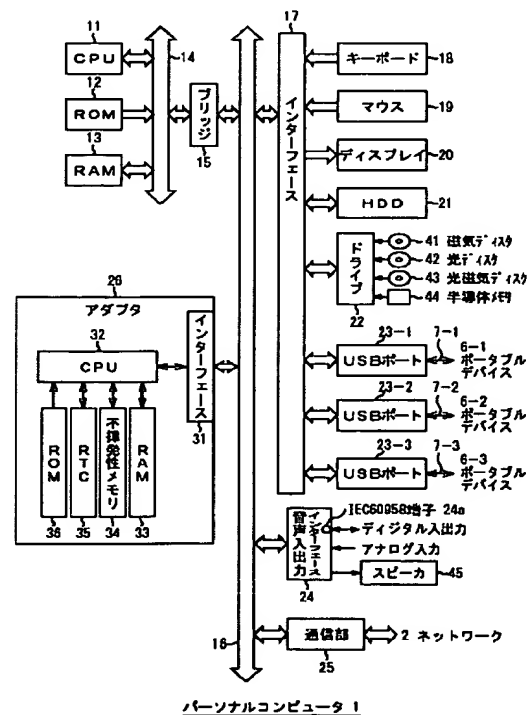
最終頁に続く

(54) 【発明の名称】 情報処理装置および方法、並びにプログラム格納媒体

(57) 【要約】

【課題】 記憶されているデータが不正に読み出され、解析されるのを防止する。

【解決手段】 CPU 11は、アダプタ26に実行させるプログラムに含まれる命令列を並び替える。CPU 11は、プログラムを暗号化する。HDD 21は、命令列が並び替えられ、暗号化されたプログラムを記録する。インターフェース17は、HDD 21に記録されているプログラムを、アダプタ7に送信する。



## 【特許請求の範囲】

【請求項 1】 半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置において、  
前記半導体 I C に実行させる前記プログラムに含まれる命令列を並び替える並び替え手段と、  
前記プログラムを暗号化する暗号化手段と、  
前記命令列が並び替えられ、暗号化された前記プログラムを記録する記録手段と、  
前記記録手段に記録されている前記プログラムを、前記半導体 I C に送信する送信手段とを含むことを特徴とする情報処理装置。

【請求項 2】 前記プログラムは、インタープリタに実行させるソースプログラムであることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 前記プログラムは、オブジェクトプログラムであることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 4】 半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置の情報処理方法において、  
前記半導体 I C に実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、  
前記プログラムを暗号化する暗号化ステップと、  
前記命令列が並び替えられ、暗号化された前記プログラムを記録する記録ステップと、  
前記記録ステップで記録されている前記プログラムを、前記半導体 I C に送信する送信ステップとを含むことを特徴とする情報処理方法。

【請求項 5】 半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置の情報処理用のプログラムであって、  
前記半導体 I C に実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、  
前記プログラムを暗号化する暗号化ステップと、  
前記命令列が並び替えられ、暗号化された前記プログラムを記録する記録ステップと、  
前記記録ステップで記録されている前記プログラムを、前記半導体 I C に送信する送信ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、情報処理装置および方法、並びにプログラム格納媒体に関し、特に、所定のデータを記憶し、所定の処理を行う情報処理装置および方法、並びにプログラム格納媒体に関する。

## 【0002】

【従来の技術】最近、CD (Compact Disk)、MD (Mini Disk) といった音楽データをデジタル式に記録または再

生することができる装置が普及してきた。その結果、このようなデジタル的に音楽データを記録再生できる装置をパーソナルコンピュータなどと組み合わせることで、デジタル音楽データを不正に複製することも比較的容易に行うことができるようになってきた。そこで、著作物としての音楽データを不正に複製することができないようにするために、各種の方法が提案されている。

【0003】例えば、コピー元を制御するソフトウェアに、コピー先の装置と相互認証させ、適正な認証結果が得られたとき、音楽データを暗号化して、コピー先の装置に転送させ、コピー先の装置において、その暗号化されたデータを復号して利用するようにすることが提案されている。

【0004】また、コピー元のソフトウェアに所定のハードウェアに記憶されている ID を利用して、コピー先の装置と相互認証させることも提案されている。

【0005】さらにまた、認証、暗号、および復号処理を、ワイアードロジックのハードウェアで実行させることも提案されている。

## 【0006】

【発明が解決しようとする課題】しかしながら、ソフトウェアだけで認証処理、暗号化処理、および復号処理を行うようにする場合、ソフトウェアを解析し、改竄することで、音楽データが不正に複製されてしまう恐れがある。

【0007】また、所定の ID をハードウェアに記憶させ、パーソナルコンピュータ上のソフトウェアにより、これを読み出し、利用させるようにする場合、読み出された ID がソフトウェアに転送される途中において読み取られ、解析、改竄されてしまう恐れがあった。

【0008】さらに、認証処理、暗号化処理、および復号処理をワイアードロジックのハードウェアにより実行するようにすると、解析や改竄は防止することが可能であるが、新たな認証処理、暗号化処理、および復号処理を行うようにするには、既存のハードウェアを新たなハードウェアと交換するか、新たなハードウェアを追加する必要が生じる。

【0009】本発明はこのような状況に鑑みてなされたものであり、記憶されているデータが不正に読み出され、解析されることを防止できるようにするものである。

## 【0010】

【課題を解決するための手段】請求項 1 に記載の情報処理装置は、半導体 I C に実行させるプログラムに含まれる命令列を並び替える並び替え手段と、プログラムを暗号化する暗号化手段と、命令列が並び替えられ、暗号化されたプログラムを記録する記録手段と、記録手段に記録されているプログラムを、半導体 I C に送信する送信手段とを含むことを特徴とする。

【0011】請求項 4 に記載の情報処理方法は、半導体

IC に実行させるプログラムに含まれる命令列を並び替える並び替えステップと、プログラムを暗号化する暗号化ステップと、命令列が並び替えられ、暗号化されたプログラムを記録する記録ステップと、記録ステップで記録されているプログラムを、半導体 IC に送信する送信ステップとを含むことを特徴とする。

【 0 0 1 2 】請求項 5 に記載のプログラム格納媒体のプログラムは、情報処理装置に、半導体 IC に実行させるプログラムに含まれる命令列を並び替える並び替えステップと、プログラムを暗号化する暗号化ステップと、命令列が並び替えられ、暗号化されたプログラムを記録する記録ステップと、記録ステップで記録されているプログラムを、半導体 IC に送信する送信ステップとを含むことを特徴とする。

【 0 0 1 3 】請求項 1 に記載の情報処理装置、請求項 4 に記載の情報処理方法、および請求項 5 に記載のプログラム格納媒体においては、半導体 IC に実行させるプログラムに含まれる命令列が並び替えられ、プログラムが暗号化され、命令列が並び替えられ、暗号化されたプログラムが記録され、記録されているプログラムが、半導体 IC に送信される。

#### 【 0 0 1 4 】

【発明の実施の形態】図 1 は、本発明に係るコンテンツデータ管理システムの一実施の形態を示す図である。パーソナルコンピュータ 1 は、ローカルエリアネットワークまたはインターネットなどから構成されるネットワーク 2 に接続されている。パーソナルコンピュータ 1 は、EMD (Electrical Music Distribution) サーバ 4 - 1 乃至 4 - 3 から受信した、または後述する CD (Compact Disc) から読み取った楽音のデータ (以下、コンテンツと称する) を、所定の圧縮の方式 (例えば、ATRAC3 (商標) ) に変換するとともに DES (Data Encryption Standard) などの暗号化方式で暗号化して記録する。

【 0 0 1 5 】パーソナルコンピュータ 1 は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。

【 0 0 1 6 】利用条件のデータは、例えば、その利用条件のデータに対応するコンテンツを同時に利用することができるポータブルデバイス (Portable Device (PD とも称する) ) の台数 (後述する、いわゆるチェックアウトできる PD の台数) を示す。利用条件のデータに示される数だけコンテンツをチェックアウトしたときでも、パーソナルコンピュータ 1 は、そのコンテンツを再生できる。

【 0 0 1 7 】または、利用条件のデータは、コピーすることができることを示す。コンテンツをポータブルデバイス 6 - 1 乃至 6 - 3 にコピーしたとき、パーソナルコンピュータ 1 は記録しているコンテンツを再生できる。コンテンツの、ポータブルデバイス 6 - 1 乃至 6 - 3 に記憶させることができる回数は、制限される場合があ

る。この場合、コピーできる回数は、増えることがない。

【 0 0 1 8 】または、利用条件のデータは、他のパーソナルコンピュータに移動することができるなどを示す。ポータブルデバイス 6 - 1 乃至 6 - 3 にコンテンツを移動させた後、パーソナルコンピュータ 1 が記録しているコンテンツは使用できなくなる (コンテンツが削除されるか、または利用条件が変更されて使用できなくなる) 。

【 0 0 1 9 】利用条件のデータの詳細は、後述する。

【 0 0 2 0 】パーソナルコンピュータ 1 は、暗号化して記録しているコンテンツを、コンテンツに関連するデータ (例えば、曲名、または再生条件など) と共に、USB (Universal Serial Bus) ケーブル 7 - 1 を介して、接続されているポータブルデバイス 6 - 1 に記憶させるとともに、ポータブルデバイス 6 - 1 に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する (以下、チェックアウトと称する) 。より詳細には、チェックアウトしたとき、パーソナルコンピュータ 1 が記録している、そのコンテンツに対応する利用条件のデータのチェックアウトできる回数は、1 減らされる。チェックアウトできる回数が 0 のとき、対応するコンテンツは、チェックアウトすることができない。

【 0 0 2 1 】パーソナルコンピュータ 1 は、暗号化して記録しているコンテンツを、コンテンツに関連するデータと共に、USB ケーブル 7 - 2 を介して、接続されているポータブルデバイス 6 - 2 に記憶させるとともに、ポータブルデバイス 6 - 2 に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する。パーソナルコンピュータ 1 は、暗号化して記録しているコンテンツを、コンテンツに関連するデータと共に、USB ケーブル 7 - 3 を介して、接続されているポータブルデバイス 6 - 3 に記憶させるとともに、ポータブルデバイス 6 - 3 に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する。

【 0 0 2 2 】また、パーソナルコンピュータ 1 は、USB ケーブル 7 - 1 を介して、接続されているポータブルデバイス 6 - 1 にパーソナルコンピュータ 1 がチェックアウトしたコンテンツを、ポータブルデバイス 6 - 1 に消去させて (または、使用できなくさせて) 、消去させたコンテンツに対応する利用条件のデータを更新する (以下、チェックインと称する) 。より詳細には、チェックインしたとき、パーソナルコンピュータ 1 が記録している、対応するコンテンツの利用条件のデータのチェックアウトできる回数は、1 増やされる。

【 0 0 2 3 】パーソナルコンピュータ 1 は、USB ケーブル 7 - 2 を介して、接続されているポータブルデバイス 6 - 2 にパーソナルコンピュータ 1 がチェックアウトし

たコンテンツを、ポータブルデバイス6-2に消去させて（または、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する。パーソナルコンピュータ1は、USBケーブル7-3を介して、接続されているポータブルデバイス6-3にパーソナルコンピュータ1がチェックアウトしたコンテンツを、ポータブルデバイス6-3に消去させて（または、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する。

【0024】パーソナルコンピュータ1は、図示せぬ他のパーソナルコンピュータがポータブルデバイス6-1にチェックアウトしたコンテンツをチェックインできない。パーソナルコンピュータ1は、他のパーソナルコンピュータがポータブルデバイス6-2にチェックアウトしたコンテンツをチェックインできない。パーソナルコンピュータ1は、他のパーソナルコンピュータがポータブルデバイス6-3にチェックアウトしたコンテンツをチェックインできない。

【0025】EMD登録サーバ3は、パーソナルコンピュータ1がEMDサーバ4-1乃至4-3からコンテンツの取得を開始するとき、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、パーソナルコンピュータ1とEMDサーバ4-1乃至4-3との相互認証に必要な認証鍵をパーソナルコンピュータ1に送信するとともに、EMDサーバ4-1乃至4-3に接続するためのプログラムをパーソナルコンピュータ1に送信する。

【0026】EMDサーバ4-1は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータ（例えば、曲名、または再生制限など）と共に、パーソナルコンピュータ1にコンテンツを供給する。EMDサーバ4-2は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータと共に、パーソナルコンピュータ1にコンテンツを供給する。EMDサーバ4-3は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータと共に、パーソナルコンピュータ1にコンテンツを供給する。

【0027】EMDサーバ4-1乃至4-3のそれぞれが供給するコンテンツは、同一または異なる圧縮の方式で圧縮されている。EMDサーバ4-1乃至4-3のそれぞれが供給するコンテンツは、同一または異なる暗号化の方式で暗号化されている。

【0028】WWW (World Wide Web) サーバ5-1は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツを読み取ったCD（例えば、CDのアルバム名、またはCDの販売会社など）、およびCDから読み取ったコンテンツに対応するデータ（例えば、曲名、または作曲者名など）をパーソナルコンピュータ1に供給する。WWWサーバ5-2は、パーソナルコンピ

ュータ1の要求に対応して、ネットワーク2を介して、コンテンツを読み取ったCD、およびCDから読み取ったコンテンツに対応するデータをパーソナルコンピュータ1に供給する。

【0029】ポータブルデバイス6-1は、パーソナルコンピュータ1から供給されたコンテンツ（すなわち、チェックアウトされたコンテンツ）を、コンテンツに関連するデータ（例えば、曲名、または再生制限など）と共に記憶する。ポータブルデバイス6-1は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。

【0030】例えば、コンテンツに関連するデータとして記憶されている、再生制限としての再生回数を超えて再生しようとしたとき、ポータブルデバイス6-1は、対応するコンテンツの再生を停止する。コンテンツに関連するデータとして記憶されている再生制限としての、再生期限を過ぎた後に再生しようとしたとき、ポータブルデバイス6-1は、対応するコンテンツの再生を停止する。

【0031】使用者は、コンテンツを記憶したポータブルデバイス6-1をパーソナルコンピュータ1から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【0032】ポータブルデバイス6-2は、パーソナルコンピュータ1から供給されたコンテンツを、コンテンツに関連するデータと共に記憶する。ポータブルデバイス6-2は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス6-2をパーソナルコンピュータ1から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【0033】ポータブルデバイス6-3は、パーソナルコンピュータ1から供給されたコンテンツを、コンテンツに関連するデータと共に記憶する。ポータブルデバイス6-3は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス6-3をパーソナルコンピュータ1から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【0034】以下、ポータブルデバイス6-1乃至6-3を個々に区別する必要がないとき、単にポータブルデバイス6と称する。

【0035】図2は、パーソナルコンピュータ1の構成を説明する図である。CPU (Central Processing Unit) 11は、各種アプリケーションプログラム（詳細につい

10

20

30

40

50

ては後述する)や、OS (Operating System)を実際に実行する。ROM (Read-only Memory) 12は、一般的には、CPU11が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM (Random-Access Memory) 13は、CPU11の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらはCPUバスなどから構成されるホストバス14により相互に接続されている。

【0036】ホストバス14は、ブリッジ15を介して、PCI (Peripheral Component Interconnect/Interface) バスなどの外部バス16に接続されている。 10

【0037】キーボード18は、CPU11に各種の指令を入力するとき、使用者により操作される。マウス19は、ディスプレイ20の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ20は、液晶表示装置またはCRT (Cathode Ray Tube) などから成り、各種情報をテキストやイメージで表示する。HDD (Hard Disk Drive) 21は、ハードディスクを駆動し、それらにCPU11によって実行するプログラムや情報を記録または再生させる。 20

【0038】ドライブ22は、装着されている磁気ディスク41、光ディスク42 (CDを含む)、光磁気ディスク43、または半導体メモリ44に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース17、外部バス16、ブリッジ15、およびホストバス14を介して接続されているRAM13に供給する。

【0039】USBポート23-1には、USBケーブル7-1を介して、ポータブルデバイス6-1が接続される。USBポート23-1は、インターフェース17、外部バス16、ブリッジ15、またはホストバス14を介して、HDD21、CPU11、またはRAM13から供給されたデータ (例えば、コンテンツまたはポータブルデバイス6-1のコマンドなどを含む) をポータブルデバイス6-1に出力する。 30

【0040】USBポート23-2には、USBケーブル7-2を介して、ポータブルデバイス6-2が接続される。USBポート23-2は、インターフェース17、外部バス16、ブリッジ15、またはホストバス14を介して、HDD21、CPU11、またはRAM13から供給されたデータ (例えば、コンテンツまたはポータブルデバイス6-2のコマンドなどを含む) をポータブルデバイス6-2に出力する。

【0041】USBポート23-3には、USBケーブル7-3を介して、ポータブルデバイス6-3が接続される。USBポート23-3は、インターフェース17、外部バス16、ブリッジ15、またはホストバス14を介して、HDD21、CPU11、またはRAM13から供給されたデータ (例えば、コンテンツまたはポータブルデバイス6-3のコマンドなどを含む) をポータブルデバイス6 50

-3に出力する。

【0042】IEC (International Electrotechnical Commission) 60958端子24aを有する音声入出力インターフェース24は、デジタル音声入出力、あるいはアナログ音声入出力のインターフェース処理を実行する。スピーカ45は、音声入出力インターフェース24から供給された音声信号を基に、コンテンツに対応する所定の音声を出力する。

【0043】これらのキーボード18乃至音声入出力インターフェース24は、インターフェース17に接続されており、インターフェース17は、外部バス16、ブリッジ15、およびホストバス14を介してCPU11に接続されている。

【0044】通信部25は、ネットワーク2が接続され、CPU11、またはHDD21から供給されたデータ (例えば、登録の要求、またはコンテンツの送信要求など) を、所定の方式のパケットに格納して、ネットワーク2を介して、送信するとともに、ネットワーク2を介して、受信したパケットに格納されているデータ (例えば、認証鍵、またはコンテンツなど) をCPU11、RAM13、またはHDD21に出力する。

【0045】半導体ICとして、一体的に形成され、パーソナルコンピュータ1に装着されるアダプタ26のCPU32は、外部バス16、ブリッジ15、およびホストバス14を介してパーソナルコンピュータ1のCPU11と共働し、各種の処理を実行する。RAM33は、CPU32が各種の処理を実行する上において必要なデータやプログラムを記憶する。不揮発性メモリ34は、パーソナルコンピュータ1の電源がオフされた後も保持する必要があるデータを記憶する。ROM36には、パーソナルコンピュータ1から、暗号化されているプログラムが転送されてきたとき、それを復号するプログラムが記憶されている。RTC (Real Time Clock) 35は、計時動作を実行し、時刻情報を提供する。

【0046】通信部25およびアダプタ26は、外部バス16、ブリッジ15、およびホストバス14を介してCPU11に接続されている。

【0047】以下、USBポート23-1乃至23-3を個々に区別する必要があるとき、単に、USBポート23と称する。以下、USBケーブル7-1乃至7-3を個々に区別する必要があるとき、単にUSBケーブル7と称する。

【0048】次に、ポータブルデバイス6の構成を図3を参照して説明する。電源回路52は、乾電池51から供給される電源電圧を所定の電圧の内部電力に変換して、CPU53乃至表示部67に供給することにより、ポータブルデバイス6全体を駆動させる。

【0049】USBコントローラ57は、USBコネクタ56を介して、パーソナルコンピュータ1とUSBケーブル7を介して接続された場合、パーソナルコンピュータ1か

ら転送されたコンテンツを含むデータを、内部バス 5 8 を介して、CPU 5 3 に供給する。

【0050】パーソナルコンピュータ 1 から転送されるデータは、1 パケット当たり 64 バイトのデータから構成され、12Mbit/sec の転送レートでパーソナルコンピュータ 1 から転送される。

【0051】ポータブルデバイス 6 に転送されるデータは、ヘッダおよびコンテンツから構成される。ヘッダには、コンテンツ ID、ファイル名、ヘッダサイズ、コンテンツ鍵、ファイルサイズ、コーデック ID、ファイル情報などが格納されていると共に、再生制限処理に必要な再生制限データ、開始日時、終了日時、回数制限、および再生回数カウンタなどが格納されている。コンテンツは、ATRAC3 などの符号化方式で符号化され、暗号化されている。

【0052】ヘッダサイズは、ヘッダのデータ長（例えば、33 バイトなど）を表し、ファイルサイズは、コンテンツのデータ長（例えば、33,636,138 バイトなど）を表す。

【0053】コンテンツ鍵は、暗号化されているコンテンツを復号するための鍵であり、パーソナルコンピュータ 1 とポータブルデバイス 6 との相互認証の処理で生成されたセッション鍵（一時鍵）を基に暗号化された状態で、パーソナルコンピュータ 1 からポータブルデバイス 6 に送信される。

【0054】ポータブルデバイス 6 が USB ケーブル 7 を介してパーソナルコンピュータ 1 の USB ポート 2 3 に接続されたとき、ポータブルデバイス 6 とパーソナルコンピュータ 1 とは、相互認証の処理を実行する。この相互認証の処理は、例えば、チャレンジレスポンス方式の認証の処理である。ちなみに、ポータブルデバイス 6 の DSP 5 9 または CPU 5 3 は、チャレンジレスポンス方式の認証の処理を行うとき、暗号解読（復号）の処理を実行する。

【0055】チャレンジレスポンス方式とは、例えば、パーソナルコンピュータ 1 が生成するある値（チャレンジ）に対して、ポータブルデバイス 6 がパーソナルコンピュータ 1 と共有している秘密鍵を使用して生成した値（レスポンス）で応答する方式である。チャレンジレスポンス方式の相互認証の処理においては、パーソナルコンピュータ 1 が生成する値は認証の処理毎に毎回変化するので、例えば、ポータブルデバイス 6 が出力した、秘密鍵を使用して生成された値が読み出されて、いわゆる、なりすましの攻撃を受けても、次の相互認証の処理では、相互認証に使用される値が異なるので、パーソナルコンピュータ 1 は不正を検出できる。

【0056】コンテンツ ID は、コンテンツに対応した、コンテンツを特定するための ID である。

【0057】コーデック ID は、コンテンツの符号化方式に対応した ID であり、例えば、コーデック ID " 1 " は、

ATRAC3 に対応し、コーデック ID " 0 " は、MP3 (MPEG (Moving Picture Experts Group) Audio Layer-3) に対応する。

【0058】ファイル名は、コンテンツに対応するパーソナルコンピュータ 1 が記録しているコンテンツファイル（後述する）を ASCII (American National Standard Code for Information Interchange) コードに変換したデータであり、ファイル情報は、コンテンツに対応する曲名、アーティスト名、作詞者名、または作曲者名などを ASCII コードに変換したデータである。

【0059】再生制限データは、コンテンツの再生が可能な期間（すなわち、開始日時または終了日時）または回数制限（再生の回数の制限）が設定されているか否かを示すデータである。再生制限データには、回数制限が設定されているとき、" 1 " が割り当てられ、再生が可能な期間が設定されているとき、" 2 " が割り当てられ、回数制限および再生が可能な期間がいずれも設定されていないとき（いわゆる、買い取りで購入されたとき）、" 0 " が割り当てられる。

【0060】開始日時および終了日時は、再生制限データが " 2 " であるとき、再生可能期間の範囲を示すデータである。例えば、開始日時が " 0 0 0 4 0 F " であり、終了日時が " 0 0 0 7 0 F " であるとき、対応するコンテンツは、2000 年 4 月 15 日から 2000 年 7 月 15 日まで、再生が可能である。

【0061】同様に、回数制限および再生回数カウンタは、再生制限データが " 1 " または " 2 " であるとき、回数制限は、そのコンテンツに対応して予め設定された再生可能な回数であり、再生回数カウンタは、そのコンテンツの再生の処理を実行したとき CPU 5 3 により更新される、コンテンツが再生された回数を示す。例えば、回数制限が " 0 2 " であるとき、そのコンテンツの再生可能な回数は 2 回であり、再生回数カウンタが " 0 1 " であるとき、そのコンテンツが再生された回数は 1 回である。

【0062】例えば、再生制限データが " 2 " であり、開始日時が " 0 0 0 4 0 F " であり、終了日時が " 0 0 0 7 0 F " であり、回数制限が " 0 2 " であるとき、ポータブルデバイス 6 は、対応するコンテンツを、2000 年 4 月 15 日から 2000 年 7 月 15 日までの期間において、1 日 2 回ずつ繰り返し再生できる。

【0063】例えば、再生制限データが " 1 " であり、開始日時が " 0 0 0 0 0 0 " であり、終了日時が " 0 0 0 0 0 0 " であり、回数制限が " 0 a " であり、再生回数カウンタが " 0 5 " であるとき、対応するコンテンツは、再生可能な期間の制限がなく、再生可能な回数が 10 回であり、再生された回数が 5 回である。

【0064】ポータブルデバイス 6 が、パーソナルコンピュータ 1 からコンテンツと共にコンテンツの書き込み命令を受信した場合、ROM 5 5 から RAM 5 4 に読み出した

10

20

30

40

50

メインプログラムを実行するCPU 5 3は、書き込み命令を受け取り、フラッシュメモリコントローラ 6 0を制御して、パーソナルコンピュータ 1から受信したコンテンツをフラッシュメモリ 6 1に書き込ませる。

【0065】フラッシュメモリ 6 1は、約64MByteの記憶容量を有し、コンテンツを記憶する。また、フラッシュメモリ 6 1には、所定の圧縮方式で圧縮されているコンテンツを伸張するための再生用コードが予め格納されている。

【0066】なお、フラッシュメモリ 6 1は、ポータブルデバイス 6にメモリカードとして着脱可能とすることができる。

【0067】使用者による、図示せぬ再生/停止ボタンの押し下げ操作に対応した再生命令が操作キーコントローラ 6 2を介してCPU 5 3に供給されると、CPU 5 3は、フラッシュメモリコントローラ 6 0に、フラッシュメモリ 6 1から、再生用コードとコンテンツとを読み出させ、DSP 5 9に転送させる。

【0068】DSP 5 9は、フラッシュメモリ 6 1から転送された再生用コードに基づいてコンテンツをCRC (Cyclic Redundancy Check) 方式で誤り検出をした後、再生して、再生したデータ (図 3 中においてD1で示す) をデジタル/アナログ変換回路 6 3に供給する。

【0069】DSP 5 9は、内部に設けられた図示せぬ発信回路とともに一体に構成され、外付けされた水晶で成る発振子 5 9 AからのマスタークロックMCLKを基に、コンテンツを再生するとともに、マスタークロックMCLK、マスタークロックMCLKを基に内部の発振回路で生成した所定の周波数のビットクロックBCLK、並びにフレーム単位のLチャンネルクロックLCLK、およびRチャンネルクロックRCLKからなる動作クロックLRCLKをデジタルアナログ変換回路 6 3に供給する。

【0070】DSP 5 9は、コンテンツを再生するとき、再生用コードに従って上述の動作クロックをデジタルアナログ変換回路 6 3に供給して、コンテンツを再生しないとき、再生用コードに従って動作クロックの供給を停止して、デジタルアナログ変換回路 6 3を停止させて、ポータブルデバイス 6全体の消費電力量を低減する。

【0071】同様に、CPU 5 3およびUSBコントローラ 5 7も、水晶でなる発振子 5 3 Aまたは5 7 Aがそれぞれ外付けされ、発振子 5 3 Aまたは5 7 Aからそれぞれ供給されるマスタークロックMCLKに基づき、所定の処理を実行する。

【0072】このように構成することで、ポータブルデバイス 6は、CPU 5 3、DSP 5 9、USBコントローラ 5 7等の各回路ブロックに対してクロック供給を行うためのクロック発生モジュールが不要となり、回路構成を簡素化すると共に小型化することができる。

【0073】デジタルアナログ変換回路 6 3は、再生

したコンテンツをアナログの音声信号に変換して、これを増幅回路 6 4に供給する。増幅回路 6 4は、音声信号を増幅して、ヘッドフォンジャック 6 5を介して、図示せぬヘッドフォンに音声信号を供給する。

【0074】このように、ポータブルデバイス 6は、図示せぬ再生/停止ボタンが押圧操作されたとき、CPU 5 3の制御に基づいてフラッシュメモリ 6 1に記憶されているコンテンツを再生するとともに、再生中に再生/停止ボタンが押圧操作されたとき、コンテンツの再生を停止する。

【0075】ポータブルデバイス 6は、停止後に再度再生/停止ボタンが押圧操作されたとき、CPU 5 3の制御に基づいて停止した位置からコンテンツの再生を再開する。再生/停止ボタンが押圧操作により再生を停止して操作が加わることなく数秒間経過したとき、ポータブルデバイス 6は、自動的に電源をオフして消費電力を低減する。

【0076】因みに、ポータブルデバイス 6は、電源がオフになった後に再生/停止ボタンが押圧操作されたとき、前回の停止した位置からコンテンツを再生せず、1曲目から再生する。

【0077】また、ポータブルデバイス 6のCPU 5 3は、LCDコントローラ 6 8を制御して、表示部 6 7に、再生モードの状態 (例えば、リピート再生、イントロ再生など)、イコライザ調整 (すなわち、音声信号の周波数帯域に対応した利得の調整)、曲番号、演奏時間、再生、停止、早送り、早戻しなどの状態、音量および乾電池 5 1の残量等の情報を表示させる。

【0078】さらに、ポータブルデバイス 6は、EEPROM 6 8に、フラッシュメモリ 8 0に書き込まれているコンテンツの数、それぞれのコンテンツが書き込まれているフラッシュメモリ 6 1のブロック位置、およびその他の種々のメモリ蓄積情報等のいわゆるFAT (File Allocation Table) を格納する。

【0079】因みに、本実施の形態においては、コンテンツは、64KByteを1ブロックとして扱われ、1曲のコンテンツに対応したブロック位置がFATに格納される。

【0080】フラッシュメモリ 6 1にFATが格納される場合、例えば、1曲目のコンテンツがCPU 5 3の制御によりフラッシュメモリ 6 1に書き込まれると、1曲目のコンテンツに対応するブロック位置がFATとしてフラッシュメモリ 6 1に書き込まれ、次に、2曲目のコンテンツがフラッシュメモリ 6 1に書き込まれると、2曲目のコンテンツに対応するブロック位置がFATとしてフラッシュメモリ 6 1 (1曲目と同一の領域) に書き込まれる。

【0081】このように、FATは、フラッシュメモリ 6 1へのコンテンツの書き込みの度に書き換えられ、更に、データの保護の為、同一のデータがリザーブ用に2重に書き込まれる。

【0082】FATがフラッシュメモリ61に書き込まれると、1回のコンテンツの書き込みに対応して、フラッシュメモリ61の同一の領域が2回書き換えられるので、少ないコンテンツの書き込みの回数で、フラッシュメモリ61に規定されている書き換えの回数に達してしまい、フラッシュメモリ61の書き換えができなくなってしまう。

【0083】そこで、ポータブルデバイス6は、FATをEEPROM68に記憶させて、1回のコンテンツの書き込みに対応するフラッシュメモリ61の書き換えの頻度を少なくしている。

【0084】書き換えの回数の多いFATをEEPROM68に記憶させることにより、FATをフラッシュメモリ61に記憶させる場合に比較して、ポータブルデバイス6は、コンテンツの書き込みができる回数を数十倍以上に増やすことができる。更に、CPU53は、EEPROM68にFATを追記するように書き込ませるので、EEPROM68の同一の領域の書き換えの頻度を少なくして、EEPROM68が短期間で書き換え不能になることを防止する。

【0085】ポータブルデバイス6は、USBケーブル7を介してパーソナルコンピュータ1に接続されたとき（以下、これをUSB接続と称する）、USBコントローラ57からCPU53に供給される割り込み信号に基づき、USB接続されたことを認識する。

【0086】ポータブルデバイス6は、USB接続されたことを認識すると、パーソナルコンピュータ1からUSBケーブル7を介して規定電流値の外部電力の供給を受けるとともに、電源回路52を制御して、乾電池51からの電力の供給を停止させる。

【0087】CPU53は、USB接続されたとき、DSP59のコンテンツの再生の処理を停止させる。これにより、CPU53は、パーソナルコンピュータ1から供給される外部電力が規定電流値を超えてしまうことを防止して、規定電流値の外部電力を常時受けられるように制御する。

【0088】このようにCPU53は、USB接続されると、乾電池51から供給される電力からパーソナルコンピュータ1から供給される電力に切り換えるので、電力単価の安いパーソナルコンピュータ1からの外部電力が使用され、電力単価の高い乾電池51の消費電力が低減され、かくして乾電池51の寿命を延ばすことができる。

【0089】なお、CPU53は、パーソナルコンピュータ1からUSBケーブル7を介して外部電力の供給を受けたとき、DSP59の再生処理を停止させることにより、DSP59からの輻射を低減させ、その結果としてパーソナルコンピュータ1を含むシステム全体の輻射を一段と低減させる。

【0090】図4は、CPU11の所定のプログラムの実行等により実現される、パーソナルコンピュータ1の機能の構成を説明するブロック図である。コンテンツ管理

プログラム111は、EMD選択プログラム131、チェックイン／チェックアウト管理プログラム132、暗号方式変換プログラム135、圧縮方式変換プログラム136、暗号化プログラム137、利用条件変換プログラム139、利用条件管理プログラム140、認証プログラム141、復号プログラム142、PD用ドライバ143、購入用プログラム144、および購入用プログラム145などの複数のプログラムで構成されている。

【0091】コンテンツ管理プログラム111は、例えば、シャッフルされているインストラクション、または暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、コンテンツ管理プログラム111を読み出しても、インストラクションを特定できないなど）ように構成されている。

【0092】EMD選択プログラム131は、コンテンツ管理プログラム111がパーソナルコンピュータ1にインストールされるとき、コンテンツ管理プログラム111には含まれず、後述するEMDの登録の処理において、ネットワーク2を介して、EMD登録サーバ3から受信される。EMD選択プログラム131は、EMDサーバ4-1乃至4-3のいずれかとの接続を選択して、購入用アプリケーション115、または購入用プログラム144若しくは142に、EMDサーバ4-1乃至4-3のいずれかとの通信（例えば、コンテンツを購入するときの、コンテンツのダウンロードなど）を実行させる。

【0093】チェックイン／チェックアウト管理プログラム132は、チェックインまたはチェックアウトの設定、およびコンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに基づいて、コンテンツファイル161-1乃至161-Nに格納されているコンテンツをポータブルデバイス6-1乃至6-3のいずれかにチェックアウトするか、またはポータブルデバイス6-1乃至6-3に記憶されているコンテンツをチェックインする。

【0094】チェックイン／チェックアウト管理プログラム132は、チェックインまたはチェックアウトの処理に対応して、コンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに格納されている利用条件のデータを更新する。

【0095】コピー管理プログラム133は、コンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに基づいて、コンテンツファイル161-1乃至161-Nに格納されているコンテンツをポータブルデバイス6-1乃至6-3のいずれかにコピーするか、またはポータブルデバイス6-1乃至6-3からコンテンツをコンテンツデータベース114にコピーする。

【0096】移動管理プログラム134は、コンテンツデータベース114に記録されている利用条件ファイル

1 6 2 - 1 乃至 1 6 2 - N に基づいて、コンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツをポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかに移動するか、またはポータブルデバイス 6 - 1 乃至 6 - 3 からコンテンツをコンテンツデータベース 1 1 4 に移動する。

【 0 0 9 7 】 暗号方式変換プログラム 1 3 5 は、ネットワーク 2 を介して、購入用アプリケーションプログラム 1 1 5 が EMD サーバ 4 - 1 から受信したコンテンツの暗号化の方式、購入用プログラム 1 4 4 が EMD サーバ 4 - 2 から受信したコンテンツの暗号化の方式、または購入用プログラム 1 4 5 が EMD サーバ 4 - 3 から受信したコンテンツの暗号化の方式を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツと同一の暗号化の方式に変換する。

【 0 0 9 8 】 また、暗号方式変換プログラム 1 3 5 は、ポータブルデバイス 6 - 1 または 6 - 3 にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス 6 - 1 または 6 - 3 が利用可能な暗号化方式に変換する。

【 0 0 9 9 】 圧縮方式変換プログラム 1 3 6 は、ネットワーク 2 を介して、購入用アプリケーションプログラム 1 1 5 が EMD サーバ 4 - 1 から受信したコンテンツの圧縮の方式、購入用プログラム 1 4 4 が EMD サーバ 4 - 2 から受信したコンテンツの圧縮の方式、または購入用プログラム 1 4 5 が EMD サーバ 4 - 3 から受信したコンテンツの圧縮の方式を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツと同一の圧縮の方式に変換する。

【 0 1 0 0 】 また、圧縮方式変換プログラム 1 3 6 は、ポータブルデバイス 6 - 1 または 6 - 3 にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス 6 - 1 または 6 - 3 が利用可能な圧縮の方式に変換する。

【 0 1 0 1 】 暗号化プログラム 1 3 7 は、例えば CD から読み取られ、録音プログラム 1 1 3 から供給されたコンテンツ（暗号化されていない）を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツと同一の暗号化の方式で暗号化する。

【 0 1 0 2 】 圧縮／伸張プログラム 1 3 8 は、例えば CD から読み取られ、録音プログラム 1 1 3 から供給されたコンテンツ（圧縮されていない）を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツと同一の符号化の方式で符号化する。圧縮／伸張プログラム 1 3 8 は、符号化されているコンテンツを伸張（復号）する。

【 0 1 0 3 】 利用条件変換プログラム 1 3 9 は、ネットワーク 2 を介して、購入用アプリケーションプログラム 1 1 5 が EMD サーバ 4 - 1 から受信したコンテンツの利用条件を示すデータ（いわゆる、Usage Rule）、購入用プログラム 1 4 4 が EMD サーバ 4 - 2 から受信したコンテンツの利用条件を示すデータ、または購入用プログラム 1 4 5 が EMD サーバ 4 - 3 から受信したコンテンツの利用条件を示すデータを、コンテンツデータベース 1 1 4 が記録している利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N に格納されている利用条件データと同一のフォーマットに変換する。

【 0 1 0 4 】 また、利用条件変換プログラム 1 3 9 は、ポータブルデバイス 6 - 1 または 6 - 3 にコンテンツをチェックアウトするとき、チェックアウトするコンテンツに対応する利用条件のデータを、ポータブルデバイス 6 - 1 または 6 - 3 が利用可能な利用条件のデータに変換する。

【 0 1 0 5 】 利用条件管理プログラム 1 4 0 は、コンテンツのコピー、移動、チェックイン、またはチェックアウトの処理を実行する前に、コンテンツデータベース 1 1 4 に記録されている利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N に格納されている利用条件のデータに対応するハッシュ値（後述する）を基に、利用条件のデータの改竄を検出する。利用条件管理プログラム 1 4 0 は、コンテンツのコピー、移動、チェックイン、またはチェックアウトの処理に伴う、コンテンツデータベース 1 1 4 に記録されている利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N に格納されている利用条件のデータを更新に対応して、利用条件のデータに対応するハッシュ値を更新する。

【 0 1 0 6 】 認証プログラム 1 4 1 は、コンテンツ管理プログラム 1 1 1 と購入用アプリケーションプログラム 1 1 5 との相互認証の処理、およびコンテンツ管理プログラム 1 1 1 と購入用プログラム 1 4 4 との相互認証の処理を実行する。また、認証プログラム 1 4 1 は、EMD サーバ 4 - 1 と購入用アプリケーションプログラム 1 1 5 との相互認証の処理、EMD サーバ 4 - 2 と購入用プログラム 1 4 4 との相互認証の処理、および EMD サーバ 4 - 3 と購入用プログラム 1 4 5 との相互認証の処理で利用される認証鍵を記憶している。

【 0 1 0 7 】 認証プログラム 1 4 1 が相互認証の処理で利用する認証鍵は、コンテンツ管理プログラム 1 1 1 がパーソナルコンピュータ 1 にインストールされたとき、認証プログラム 1 4 1 に記憶されておらず、表示操作指示プログラム 1 1 2 により登録の処理が正常に実行されたとき、EMD 登録サーバ 3 から供給され、認証プログラム 1 4 1 に記憶される。

【 0 1 0 8 】 復号プログラム 1 4 2 は、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツをパ

ーソナルコンピュータ 1 が再生するとき、コンテンツを復号する。

【0109】PD用ドライバ 143 は、ポータブルデバイス 6-2 に所定のコンテンツをチェックアウトするとき、またはポータブルデバイス 6-2 から所定のコンテンツをチェックインするとき、ポータブルデバイス 6-2 にコンテンツまたはポータブルデバイス 6-2 に所定の処理を実行させるコマンドを供給する。

【0110】PD用ドライバ 143 は、ポータブルデバイス 6-1 に所定のコンテンツをチェックアウトするとき、またはポータブルデバイス 6-1 から所定のコンテンツをチェックインするとき、デバイスドライバ 116-1 にコンテンツ、またはデバイスドライバ 116-1 に所定の処理を実行させるコマンドを供給する。

【0111】PD用ドライバ 143 は、ポータブルデバイス 6-3 に所定のコンテンツをチェックアウトするとき、またはポータブルデバイス 6-3 から所定のコンテンツをチェックインするとき、デバイスドライバ 116-2 にコンテンツ、またはデバイスドライバ 116-2 に所定の処理を実行させるコマンドを供給する。

【0112】購入用プログラム 144 は、いわゆる、プラグインプログラムであり、コンテンツ管理プログラム 111 と共にインストールされ、EMD登録サーバ 3 からネットワーク 2 を介して供給され、または所定のCDに記録されて供給される。購入用プログラム 144 は、パーソナルコンピュータ 1 にインストールされたとき、コンテンツ管理プログラム 111 の有する所定の形式のインターフェースを介して、コンテンツ管理プログラム 111 とデータを送受信する。

【0113】購入用プログラム 144 は、例えば、シャッフルされているインストラクション、または暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、購入用プログラム 144 を読み出しても、インストラクションを特定できないなど）ように構成されている。

【0114】購入用プログラム 144 は、ネットワーク 2 を介して、EMDサーバ 4-2 に所定のコンテンツの送信を要求するとともに、EMDサーバ 4-2 からコンテンツを受信する。また、購入用プログラム 144 は、EMDサーバ 4-2 からコンテンツを受信するとき、課金の処理を実行する。

【0115】購入用プログラム 145 は、コンテンツ管理プログラム 111 と共にインストールされるプログラムであり、ネットワーク 2 を介して、EMDサーバ 4-3 に所定のコンテンツの送信を要求するとともに、EMDサーバ 4-3 からコンテンツを受信する。また、購入用プログラム 145 は、EMDサーバ 4-3 からコンテンツを受信するとき、課金の処理を実行する。

【0116】表示操作指示プログラム 112 は、フィル

タリングデータファイル 181、表示データファイル 182、画像ファイル 183-1 乃至 183-K、または履歴データファイル 184 を基に、ディスプレイ 20 に所定のウィンドウの画像を表示させ、キーボード 18 またはマウス 19 への操作を基に、コンテンツ管理プログラム 111 にチェックインまたはチェックアウトなどの処理の実行を指示する。

【0117】フィルタリングデータファイル 181 は、コンテンツデータベース 114 に記録されているコンテンツファイル 161-1 乃至 161-N に格納されているコンテンツそれぞれに重み付けをするためのデータを格納して、HDD 21 に記録されている。

【0118】表示データファイル 182 は、コンテンツデータベース 114 に記録されているコンテンツファイル 161-1 乃至 161-N に格納されているコンテンツに対応するデータを格納して、HDD 21 に記録されている。

【0119】画像ファイル 183-1 乃至 183-K は、コンテンツデータベース 114 に記録されているコンテンツファイル 161-1 乃至 161-N に対応する画像、または後述するパッケージに対応する画像を格納して、HDD 21 に記録されている。

【0120】以下、画像ファイル 183-1 乃至 183-K を個々に区別する必要がないとき、単に、画像ファイル 183 と称する。

【0121】履歴データファイル 184 は、コンテンツデータベース 114 に記録されているコンテンツファイル 161-1 乃至 161-N に格納されているコンテンツがチェックアウトされた回数、チェックインされた回数、その日付などの履歴データを格納して、HDD 21 に記録されている。

【0122】表示操作指示プログラム 112 は、登録の処理のとき、ネットワーク 2 を介して、EMD登録サーバ 3 に、予め記憶しているコンテンツ管理プログラム 111 のIDを送信するとともに、EMD登録サーバ 3 から認証用鍵およびEMD選択プログラム 131 を受信して、コンテンツ管理プログラム 111 に認証用鍵およびEMD選択プログラム 131 を供給する。

【0123】録音プログラム 113 は、所定のウィンドウの画像を表示させて、キーボード 18 またはマウス 19 への操作を基に、ドライブ 22 に装着された光ディスク 42 であるCDからコンテンツの録音時間などのデータを読み出す。

【0124】録音プログラム 113 は、CDに記録されているコンテンツの録音時間などを基に、ネットワーク 2 を介して、WWWサーバ 5-1 または 5-2 にCDに対応するデータ（例えば、アルバム名、またはアーティスト名など）またはCDに記録されているコンテンツに対応するデータ（例えば、曲名など）の送信を要求するとともに、WWWサーバ 5-1 または 5-2 からCDに対応するデ

ータまたはCDに記録されているコンテンツに対応するデータを受信する。

【0125】録音プログラム113は、受信したCDに対応するデータまたはCDに記録されているコンテンツに対応するデータを、表示操作指示プログラム112に供給する。

【0126】また、録音の指示が入力されたとき、録音プログラム113は、ドライブ22に装着された光ディスク42であるCDからコンテンツを読み出して、コンテンツ管理プログラム111に出力する。

【0127】コンテンツデータベース114は、コンテンツ管理プログラム111から供給された所定の方式で圧縮され、所定の方式で暗号化されているコンテンツを、コンテンツファイル161-1乃至161-Nのいずれかに格納する（HDD21に記録する）。コンテンツデータベース114は、コンテンツファイル161-1乃至161-Nにそれぞれ格納されているコンテンツに対応する利用条件のデータを、コンテンツが格納されているコンテンツファイル161-1乃至161-Nにそれぞれ対応する利用条件ファイル162-1乃至162-Nのいずれかに格納する（HDD21に記録する）。

【0128】コンテンツデータベース114は、コンテンツファイル161-1乃至161-Nまたは利用条件ファイル162-1乃至162-Nをレコードとして記録してもよい。

【0129】例えば、コンテンツファイル161-1に格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル162-1に格納されている。コンテンツファイル161-Nに格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル162-Nに格納されている。

【0130】なお、利用条件ファイル162-1乃至162-Nに記録されているデータは、後述する期限データベースに記録されているデータ、または曲データベースに記録されているデータに対応する。すなわち、コンテンツデータベース114は、後述する期限データベースおよび曲データベースを包含して、構成されている。

【0131】以下、コンテンツファイル161-1乃至161-Nを個々に区別する必要がないとき、単に、コンテンツファイル161と称する。以下、利用条件ファイル162-1乃至162-Nを個々に区別する必要がないとき、単に、利用条件ファイル162と称する。

【0132】購入用アプリケーションプログラム115は、EMD登録サーバ3からネットワーク2を介して供給され、または所定のCD-ROMに記録されて供給される。購入用アプリケーションプログラム115は、ネットワーク2を介して、EMDサーバ4-1に所定のコンテンツの送信を要求するとともに、EMDサーバ4-1からコンテンツを受信して、コンテンツ管理プログラム111に供給する。また、購入用アプリケーションプログラム11

5は、EMDサーバ4-1からコンテンツを受信するとき、課金の処理を実行する。

【0133】次に、表示データファイル82に格納されているデータとコンテンツデータベースに格納されているコンテンツファイル161-1乃至161-Nとの対応付けについて説明する。

【0134】コンテンツファイル161-1乃至161-Nのいずれかに格納されているコンテンツは、所定のパッケージに属する。パッケージは、より詳細には、オリジナルパッケージ、マイセレクトパッケージ、またはフィルタリングパッケージのいずれかである。

【0135】オリジナルパッケージは、1以上のコンテンツが属し、EMDサーバ4-1乃至4-3におけるコンテンツの分類（例えば、いわゆるアルバムに対応する）、または一枚のCDに対応する。コンテンツは、いずれかのオリジナルパッケージに属し、複数のオリジナルパッケージに属することができない。また、コンテンツが属するオリジナルパッケージは、変更することができない。使用者は、オリジナルパッケージに対応する情報の一部を編集（情報の追加、または追加した情報の変更）することができる。

【0136】マイセレクトパッケージは、使用者が任意に選択した1以上のコンテンツが属する。マイセレクトパッケージにいずれのコンテンツが属するかは、使用者が任意に編集することができる。コンテンツは、1以上のマイセレクトパッケージに同時に属することができる。また、コンテンツは、いずれのマイセレクトパッケージに属しなくともよい。

【0137】フィルタリングパッケージには、フィルタリングデータファイル181に格納されているフィルタリングデータを基に選択されたコンテンツが属する。フィルタリングデータは、EMDサーバ4-1乃至4-3またはWWWサーバ5-1若しくは5-2などからネットワーク2を介して供給され、または所定のCDに記録されて供給される。使用者は、フィルタリングデータファイル181に格納されているフィルタリングデータを編集することができる。

【0138】フィルタリングデータは、所定のコンテンツを選択する、またはコンテンツに対応する重みを算出する基準となる。例えば、今週のJ-POP（日本のポップス）ベストテンに対応するフィルタリングデータを利用すれば、パーソナルコンピュータ1は、今週の日本のポップス1位のコンテンツ乃至今週の日本のポップス10位のコンテンツを特定することができる。

【0139】フィルタリングデータファイル181は、例えば、過去1月間にチェックアウトされていた期間が長い順にコンテンツを選択するフィルタリングデータ、過去半年間にチェックアウトされた回数が多いコンテンツを選択するフィルタリングデータ、または曲名に“愛”の文字が含まれているコンテンツを選択するフィル

タリングデータなどを含んでいる。

【0140】このようにフィルタリングパッケージのコンテンツは、コンテンツに対応するコンテンツ用表示データ221（コンテンツ用表示データ221に使用者が設定したデータを含む）、または履歴データ184などと、フィルタリングデータとを対応させて選択される。

【0141】ドライバ117は、コンテンツ管理プログラム111などの制御の基に、音声入出力インターフェース24を駆動して、外部から供給されたデジタルデータであるコンテンツを入力してコンテンツ管理プログラム111に供給するか、若しくはコンテンツ管理プログラム111を介してコンテンツデータベース114から供給されたコンテンツをデジタルデータとして出力するか、または、コンテンツ管理プログラム111を介してコンテンツデータベース114から供給されたコンテンツに対応するアナログ信号を出力する。

【0142】図5は、表示操作指示プログラム112を起動させたとき、操作指示プログラム112がディスプレイ20に表示させる表示操作指示ウィンドウの例を示す図である。

【0143】表示操作指示ウィンドウには、録音プログラム113を起動させるためのボタン201、EMD選択プログラム131を起動させるためのボタン202、チェックインまたはチェックアウトの処理の設定を行うフィールドを表示させるためのボタン203、マイセレクトパッケージを編集するためフィールドを表示させるためのボタン204等が配置されている。

【0144】ボタン205が選択されているとき、フィールド211には、オリジナルパッケージに対応するデータが表示される。ボタン206が選択されているとき、フィールド211には、マイセレクトパッケージに対応するデータが表示される。ボタン207が選択されているとき、フィールド211には、フィルタリングパッケージに対応するデータが表示される。

【0145】フィールド211に表示されるデータは、パッケージに関するデータであり、例えば、パッケージ名称、またはアーティスト名などである。

【0146】例えば、図5においては、パッケージ名称”ファースト”およびアーティスト名”A太郎”、およびパッケージ名称”セカンド”およびアーティスト名”A太郎”などがフィールド211に表示される。

【0147】フィールド212には、フィールド211で選択されているパッケージに属するコンテンツに対応するデータが表示される。フィールド212に表示されるデータは、例えば、曲名、演奏時間、またはチェックアウト可能回数などである。

【0148】例えば、図5においては、パッケージ名称”セカンド”に対応するパッケージが選択されているので、パッケージ名称”セカンド”に対応するパッケージに属するコンテンツに対応する曲名”南の酒場”およ

びチェックアウト可能回数（例えば、8分音符の1つがチェックアウト1回に相当し、8分音符が2つでチェックアウト2回を示す）、並びに曲名”北の墓場”およびチェックアウト可能回数（8分音符が1つでチェックアウト1回を示す）などがフィールド212に表示される。

【0149】このように、フィールド212に表示されるチェックアウト可能回数としての1つの8分音符は、対応するコンテンツが1回チェックアウトできることを示す。

【0150】フィールド212に表示されるチェックアウト可能回数としての休符は、対応するコンテンツがチェックアウトできない（チェックアウト可能回数が0である。（ただし、パーソナルコンピュータ1はそのコンテンツを再生することができる。））ことを示す。また、フィールド212に表示されるチェックアウト可能回数としてのト音記号は、対応するコンテンツのチェックアウトの回数に制限が無い（何度でも、チェックアウトできる）ことを示している。

【0151】なお、チェックアウト可能回数は、図5に示すように所定の図形（例えば、円、星、月などでもよい）の数で表示するだけでなく、数字等で表示してもよい。

【0152】また、表示操作指示ウィンドウには、選択されているパッケージまたはコンテンツに対応付けられている画像等（図4の画像ファイル183-1乃至183-Kのいずれかに対応する）を表示させるフィールド208が配置されている。ボタン209は、選択されているコンテンツを再生する（コンテンツに対応する音声スピーカ45に出力させる）とき、クリックされる。

【0153】ボタン205が選択され、フィールド211に、オリジナルパッケージに対応するデータが表示されている場合、フィールド212に表示されている所定のコンテンツの曲名を選択して、消去の操作をしたとき、表示操作指示プログラム112は、コンテンツ管理プログラム111に、選択されている曲名に対応する、コンテンツデータベース114に格納されている所定のコンテンツを消去させる。

【0154】録音プログラム113が表示させるウィンドウのボタン（後述するボタン255）が選択されて（アクティブにされて）いる場合、CDから読み出したコンテンツがコンテンツデータベース114に記録されたとき、表示操作指示プログラム112は、表示操作指示ウィンドウに、予め指定されているポータブルデバイス6-1乃至6-3のいずれかに記憶されているコンテンツの曲名を表示するフィールド213を表示する。

【0155】録音プログラム113が表示させるウィンドウのボタンが選択されている場合、CDから読み出したコンテンツがコンテンツデータベース114に記録されたとき、表示操作指示プログラム112は、コンテン

10

20

30

40

50

ツ管理プログラム 111 に、コンテンツデータベース 114 に記録した、CD から読み出したコンテンツを予め指定されているポータブルデバイス 6-1 乃至 6-3 のいずれかにチェックアウトさせる。

【0156】フィールド 213 にはコンテンツの曲名に対応させて、フィールド 213 の最も左に、そのコンテンツがパーソナルコンピュータ 1 にチェックインできるか否かを示す記号が表示される。例えば、フィールド 213 の最も左に位置する“○”は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ 1 にチェックインできる（すなわち、パーソナルコンピュータ 1 からチェックアウトされた）ことを示している。フィールド 213 の最も左に位置する“×”は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ 1 にチェックインできない（すなわち、パーソナルコンピュータ 1 からチェックアウトされていない、例えば、他のパーソナルコンピュータからチェックアウトされた）ことを示している。

【0157】表示操作指示プログラム 112 が表示操作指示ウィンドウにフィールド 213 を表示させたとき、表示操作指示プログラム 112 は、表示操作指示ウィンドウに、予め指定されているポータブルデバイス 6-1 乃至 6-3 のいずれかに記憶されているコンテンツが属するポータブルパッケージ（ポータブルデバイス 6-1 乃至 6-3 のいずれかに記憶されているコンテンツが属するパッケージ）の名称を表示するフィールド 214、フィールド 213 を閉じるためのボタン 210、およびチェックインまたはチェックアウトを実行させるボタン 215 を表示する。

【0158】更に、表示操作指示プログラム 112 が表示操作指示ウィンドウにフィールド 213 を表示させたとき、表示操作指示プログラム 112 は、表示操作指示ウィンドウに、フィールド 212 で選択された曲名に対応するコンテンツのチェックアウトを設定するボタン 216、フィールド 213 で選択された曲名に対応するコンテンツのチェックインを設定するボタン 217、フィールド 213 に表示されたコンテンツ名に対応する全てのコンテンツのチェックインを設定するボタン 218、およびチェックインまたはチェックアウトの設定を取り消すボタン 219 を配置させる。

【0159】ボタン 216 乃至 219 の操作によるチェックインまたはチェックアウトの設定だけでは、パーソナルコンピュータ 1 は、チェックインまたはチェックアウトの処理を実行しない。

【0160】ボタン 216 乃至 219 の操作によるチェックインまたはチェックアウトの設定をした後、ボタン 215 がクリックされたとき、表示操作指示プログラム 112 は、コンテンツ管理プログラム 111 にチェックインまたはチェックアウトの処理を実行させる。すなわち、ボタン 215 がクリックされたとき、表示操作指示

プログラム 112 は、チェックインまたはチェックアウトの設定に基づき、コンテンツ管理プログラム 111 に、ポータブルデバイス 6-1 乃至 6-3 のいずれかにコンテンツを送信させるか、またはチェックインに対応する所定のコマンド（例えば、ポータブルデバイス 6-1 乃至 6-3 のいずれかが記憶している所定のコンテンツを消去させるコマンドなど）を送信させるとともに、送信したコンテンツまたはコマンドに対応する利用条件ファイル 162 に格納されている利用条件のデータを更新させる。

【0161】チェックインまたはチェックアウトが実行されたとき、表示操作指示プログラム 112 は、送信したコンテンツまたは送信されたコマンドに対応して、履歴データファイル 184 に格納されている履歴データを更新する。履歴データは、チェックインまたはチェックアウトされたコンテンツを特定する情報、またはそのコンテンツがチェックインまたはチェックアウトされた日付、そのコンテンツがチェックアウトされたポータブルデバイス 6-1 乃至 6-3 の名称などから成る。

【0162】チェックインまたはチェックアウトの設定の処理は短時間で実行できるので、使用者は、チェックインまたはチェックアウトの処理の実行後の状態を迅速に知ることができ、時間のかかるチェックインまたはチェックアウトの処理の回数を減らして、チェックインまたはチェックアウトに必要な時間全体（設定および実行を含む）を短くすることができる。

【0163】図 6 は、録音プログラム 113 がディスプレイ 20 に表示させるウィンドウの例を説明する図である。例えば、WWW サーバ 5-2 から受信した CD の情報を基に、録音プログラム 113 は、フィールド 251 に、“アシンクロナイズド”などの CD のタイトルを表示する。WWW サーバ 5-2 から受信した CD の情報を基に、録音プログラム 113 は、フィールド 252 に、例えば、“クワイ”などのアーティスト名を表示する。

【0164】WWW サーバ 5-2 から受信した CD の情報を基に、録音プログラム 113 は、フィールド 253 の曲名を表示する部分に、例えば、“ヒート”、“プラネット”、“ブラック”、“ソウル”などの曲名を表示する。同様に、録音プログラム 113 は、フィールド 253 のアーティストを表示する部分に、例えば、“クワイ”などのアーティスト名を表示する。

【0165】録音プログラム 113 が所定の CD の情報を受信した後、録音プログラム 113 は、HDD 21 の所定のディレクトリに CD の情報を格納する。

【0166】ボタン 254 などがクリックされて、CD の情報の取得の指示を受けたとき、録音プログラム 113 は、始めに、HDD 21 の所定のディレクトリを検索する。録音プログラム 113 は、そのディレクトリに CD の情報が格納されているとき、図示せぬダイアログボックスを表示して、使用者にディレクトリに格納されている

10

20

30

40

50

CDの情報を利用するか否かを選択させる。

【0167】録音プログラム113が表示させるウィンドウに配置されているコンテンツの録音の開始を指示するボタン256がクリックされたとき、録音プログラム113は、ドライブ22に格納されているCDからコンテンツを読み出して、CDから読み出したコンテンツをCDの情報と共にコンテンツ管理プログラム111に供給する。コンテンツ管理プログラム111の圧縮／伸張プログラム138は、録音プログラム113から供給されたコンテンツを所定の圧縮の方式で圧縮して、暗号化プログラム137は、圧縮されたコンテンツを、暗号化する。また、利用条件変換プログラム139は、圧縮され、暗号化されたコンテンツに対応する利用条件のデータを生成する。

【0168】コンテンツ管理プログラム111は、圧縮され、暗号化されたコンテンツを利用条件のデータと共に、コンテンツデータベース114に供給する。

【0169】コンテンツデータベース114は、コンテンツ管理プログラム111から受信したコンテンツに対応するコンテンツファイル161および利用条件ファイル162を生成して、コンテンツファイル161にコンテンツを格納するとともに、利用条件ファイル162に利用条件のデータを格納する。

【0170】コンテンツ管理プログラム111は、コンテンツデータベース114にコンテンツおよびコンテンツに対応する利用条件のデータが格納されたとき、録音プログラム113から受信したCDの情報および利用条件のデータを表示操作指示プログラム112に供給する。

【0171】表示操作指示プログラム112は、録音の処理でコンテンツデータベース114に格納されたコンテンツに対応する利用条件のデータおよびCDの情報を基に、表示データファイル182に格納する表示用のデータを生成する。

【0172】録音プログラム113が表示させるウィンドウには、更に、CDから読み出したコンテンツをコンテンツデータベース114に記録したとき、自動的に、CDから読み出したコンテンツをポータブルデバイス6-1乃至6-3のいずれかにチェックアウトさせるか否かの設定を行うボタン255が配置されている。

【0173】例えば、ボタン255がクリックされたとき、録音プログラム113は、ポータブルデバイス6-1乃至6-3のリストを示すプルダウンメニューを表示する。使用者が、そのプルダウンメニューからポータブルデバイス6-1乃至6-3のいずれかを選択したとき、パーソナルコンピュータ1は、選択されたポータブルデバイス6-1乃至6-3のいずれかに、自動的に、CDから記録したコンテンツをチェックアウトする。使用者が、そのプルダウンメニューから”チェックアウトしない”を選択した場合、パーソナルコンピュータ1は、CDからコンテンツを記録したとき、チェックアウトしな

い。

【0174】このように、録音プログラム113が表示させるウィンドウのボタン255をアクティブにしておくだけで、CDから読み出したコンテンツがコンテンツデータベース114に記録されたとき、パーソナルコンピュータ1は、予め指定されているポータブルデバイス6-1乃至6-3のいずれかに、CDから読み出したコンテンツをチェックアウトさせることができる。

【0175】次に、図7のフローチャートを参照して、コンテンツ管理プログラム111、表示操作指示プログラム112、録音プログラム113、およびコンテンツデータベース114を実行するCPU11による、ドライブ22に装着されたCDから再生したコンテンツをHDD21に転送し、コピーする場合の処理について説明する。使用者がキーボード18またはマウス19を操作して、インタフェース17を介してCPU11に対してドライブ22に装着されたCD（図示せず）から再生されたコンテンツをHDD21に転送、コピーする指令を入力すると、録音プログラム113は、ステップS11において、インタフェース17を介してディスプレイ20にコピーするコンテンツを選択するための、例えば、図6に示すGUI (Graphical User Interface) を表示させる。

【0176】具体的には、例えば、録音プログラム113は、ドライブ22に装着されたCDのTOC (Table Of Contents) を読み込み、そのCDに含まれるコンテンツの情報を得て、ディスプレイ20に表示させる。または、録音プログラム113は、CDに含まれている各コンテンツ毎のISRC (International Standard Recording Code) を読み出し、そのコンテンツの情報を得て、ディスプレイ20に表示させる。あるいはまた、ボタン254がクリックされたとき、録音プログラム113は、ネットワーク2を介してWWWサーバ5-1または5-2にアクセスし、TOCを用いて、そのCDのコンテンツの情報を得て、コンテンツに対応する曲名などをフィールド253に表示させる。

【0177】使用者は、ディスプレイ20のGUIを利用してキーボード18またはマウス19を操作し、フィールド253に表示されている曲名に対応するチェックボックスをクリックするなどして、コピーするコンテンツを選択する。

【0178】次に、ステップS12において、録音プログラム113は、利用条件管理プログラム140に、HDD21に格納されている期限データベース（図4に示すコンテンツデータベース114の利用条件ファイル162-1乃至162-Nに対応する）をチェックさせる。この期限データベースチェック処理の詳細は、図8のフローチャートに示されている。

【0179】ステップS31において利用条件管理プログラム140は、アダプタ26のCPU32と共働して、期限データベース全体のハッシュ値を計算し、ステップ

S 3 2において、その計算された値と、前回保存しておいたハッシュ値と比較する。

【0180】なお、期限データベースにデータが何ら記録されていないとき、利用条件管理プログラム140は、ハッシュ値を計算しない。

【0181】すなわち、HDD 21には、期限データベースが形成されており、この期限データベースには、図9に示すように、HDD 21に記録されているコンテンツ

(コンテンツ)を管理する管理情報として、過去に記録されたことのあるコンテンツのISRCとコピー日時が対応して記憶されている。この例においては、アイテム1乃至アイテム3の3つのアイテムについて、それぞれのISRCとコピー日時が記憶されている。この期限データベースに記録されている全てのコンテンツのISRCとコピー日時に基づいた期限データベース全体のハッシュ値が、後述するように、ステップS 38において、アダプタ26のCPU 32により計算され、不揮発性メモリ34に記憶されている。ハッシュ値は、データに対してハッシュ関数を適用して得られた値である。

【0182】ハッシュ関数は、任意の長さのメッセージを固定長に短く圧縮した値にマップする一方向性の関数であり、圧縮したデータからもとのデータを求める逆変換が困難な性質を持つものである。また、ハッシュ値同士の衝突が起こりにくく、即ち、例えば違う二つのメッセージに対して同じ値を付けることを困難にするものである。ハッシュ関数は、メッセージが通信途中で改竄されなかったことを確認するためのチェックサムとして用いられ、デジタル署名の中で用いられる。ハッシュ関数の例としては、SHA (Secure Hash Algorithm), MD (Message Digest) 5などがある。

【0183】利用条件管理プログラム140は、ステップS 31において、CPU 32が実行したのと同様にハッシュ値を計算する。そして、ステップS 32において、利用条件管理プログラム140は、CPU 32に、不揮発性メモリ34に記憶されているハッシュ値の読み出しを要求し、転送を受けたハッシュ値と、ステップS 31で、いま自分自身が計算したハッシュ値とを比較する。

【0184】ステップS 33において、利用条件管理プログラム140は、ステップS 31でいま計算したハッシュ値と、不揮発性メモリ34に記憶されている前回の期限データベースのハッシュ値とが一致するかどうかを判定し、一致しない場合には、期限データベースが改竄されたものと判定し、利用条件管理プログラム140は、ステップS 34において、例えば、録音プログラム113に「期限データベースが改竄されたので、コピーができません」といったメッセージを発生させ、インタフェース17を介してディスプレイ20に出力させ、表示させ、以後、処理を終了させる。すなわち、この場合には、CDに記録されているコンテンツを再生し、HDD 21にコピーする処理が禁止される。

【0185】ステップS 31で計算したハッシュ値と、前回のハッシュ値とが一致する場合には、ステップS 35に進み、利用条件管理プログラム140は、録音プログラム113に、ステップS 11で指定されたコピーするコンテンツとして選択されたコンテンツ(選択されたコンテンツ)のISRCをCDから取得させる。CDにISRCが記録されていない場合、利用条件管理プログラム140は、録音プログラム113に、そのCDのTOCのデータを読み出させ、そのデータにハッシュ関数を適用するなどして、例えば、58ビットなどの適当な長さのデータを得て、これをISRCに代えて用いる。

【0186】ステップS 36において、利用条件管理プログラム140は、ステップS 35で取得したISRC(すなわち、選択されたコンテンツ)が期限データベース(図9)に登録されているか否かを判定する。ISRCが期限データベースに登録されていない場合には、そのコンテンツはまだHDD 21に記録されていないことになるので、ステップS 37に進み、利用条件管理プログラム140は、そのコンテンツのISRCと現在の日時とを期限データベースに登録する。なお、利用条件管理プログラム140は、この現在の日時として、CPU 32から転送を受けた、アダプタ26のRTC 35が出力する値を利用する。そして、ステップS 38において、利用条件管理プログラム140は、その時点における期限データベースのデータを読み出し、アダプタ26のCPU 32に転送する。CPU 32は、転送されてきたデータのハッシュ値を計算し、不揮発性メモリ34に保存してする。上述したように、このようにして保存されたハッシュ値が、ステップS 32において、前回保存しておいたハッシュ値として利用される。

【0187】次に、ステップS 39において、利用条件管理プログラム140は、選択されたコンテンツが期限データベースに登録されていないことを表す未登録のフラグを設定する。このフラグは、後述する図7のステップS 13において、選択されたコンテンツが期限データベースに登録されているか否かの判定を行うときに用いられる。

【0188】ステップS 36において、選択されたコンテンツのISRCが期限データベースに登録されていると判定された場合、その選択されたコンテンツは、少なくとも一度、HDD 21に登録されたことがあるコンテンツであるということになる。そこで、この場合、ステップS 40に進み、利用条件管理プログラム140は、期限データベースに登録されているその選択されたコンテンツの登録日時より、現在の日時(アダプタ26のRTC 35が出力した現在の日時)が48時間以上経過しているかどうかを判定する。現在時刻が、登録日時より、既に48時間以上経過している場合には、HDD 21に、少なくとも一度は記録したことがあるが、既に、その時から48時間以上経過しているため、そのコンテンツを再度コピ

一させたととしても、コンテンツの大量のコピーは実質的に不可能なので、この場合には、HDD 21 へのコピーが許容される。そこで、ステップ S 41 に進み、利用条件管理プログラム 140 は、期限データベースの日時を、過去の登録日時から現在の日時（RTC 35 の出力する日時）に変更させる。そして、ステップ S 38 に戻り、利用条件管理プログラム 140 は、再び、期限データベース全体のハッシュ値を CPU 32 に計算させ、不揮発性メモリ 34 に保存させるとともに、ステップ S 39 において、そのコンテンツに対して未登録のフラグを設定する。

【0189】一方、ステップ S 40 において、現在時刻が登録日時より、まだ 48 時間以上経過していないと判定された場合、その選択されたコンテンツの HDD 21 へのコピーが禁止される。そこで、この場合には、ステップ S 42 に進み、利用条件管理プログラム 140 は、その選択されたコンテンツに対応して登録済みのフラグを設定する。

【0190】ステップ S 40 の処理により、所定の時間が経過しなければ、コンテンツの新たなコピーを生成できないので、不正でない通常の使用を目的としたコンテンツのコピーの生成を不当に妨げることなく、例えば、不正な販売または配布などに必要な大量のコンテンツのコピーの生成は、実質的に不可能となる。なお、ステップ S 40 においては、判定の基準は 48 時間以上の経過としたが、48 時間に限らず、例えば、12 時間乃至 168 時間のいずれかの時間であればよい。

【0191】以上のようにして、期限データベースチェック処理により、選択されたコンテンツが HDD 21 に登録されているか否かを表すフラグが設定される。

【0192】図 7 に戻り、ステップ S 13 においてコピー管理プログラム 133 は、選択されたコンテンツが期限データベースに登録済みであるか否かを、上述したフラグから判定する。選択されたコンテンツが登録済みである場合には、ステップ S 14 に進み、コピー管理プログラム 133 は、録音プログラム 113 に、例えば、「この曲は一度コピーされてからまだ 48 時間以上経過していないので、コピーすることができません」のようなメッセージをディスプレイ 20 に表示させる。これにより、使用者は、そのコンテンツを HDD 21 にコピーすることができない理由を知ることができる。

【0193】ステップ S 13 において、選択したコンテンツが期限データベースに登録されていないと判定された場合、ステップ S 15 に進み、録音プログラム 113 は、ドライブ 22 を制御し、そこに装着されている CD からコンテンツを読み出させる。このコンテンツには、図 10 に示すように、所定の位置にウォータマークコードが挿入されている。録音プログラム 113 は、ステップ S 16 において、コンテンツに含まれているウォータマークコードを抽出し、そのウォータマークコードがコピ

ー禁止を表しているか否かをステップ S 17 において判定する。ウォータマークコードがコピー禁止を表している場合には、ステップ S 18 に進み、コピー管理プログラム 133 は、録音プログラム 113 に例えば、「コピーは禁止されています」のようなメッセージをインタフェース 17 を介してディスプレイ 20 に表示させ、コピー処理を終了させる。

【0194】これに対して、ステップ S 17 において、ウォータマークがコピー禁止を表していないと判定された場合、ステップ S 19 に進み、録音プログラム 113 は、コンテンツを、圧縮／伸張プログラム 138 に、例えば、ATRAC (Adaptive Transform Acoustic Coding) 3 (商標) などの方式で、ソフトウェア処理により圧縮させる。ステップ S 20 において、録音プログラム 113 は、暗号化プログラム 137 に、予め設定され、メモリ 13 に記憶されている暗号鍵を用いて、例えば、DES (Data Encryption Standard) 方式、FEAL (Fast Encryption Algorithm) 方式などの暗号化方法により、コンテンツを暗号化させる。暗号鍵は、この他、例えば、ソフトウェアにより発生した乱数、あるいはアダプタ 26 の CPU 32 により発生させた乱数に基づいて生成したものをを用いることもできる。このように、パーソナルコンピュータ 1 だけではなく、それに付随して装着されたハードウェアとしてのアダプタ 26 の CPU 32 と、共働して暗号化処理を実行するようにすることで、解読がより困難となる暗号化を行うことが可能となる。

【0195】次に、ステップ S 21 において、録音プログラム 113 は、暗号化されたデータを、コンテンツデータベース 114 に転送し、1つのファイル（コンテンツファイル 161 として）としてファイル名を付けて HDD 21 に保存させる。あるいはまた、1つのファイルの一部として、そのファイル名の位置情報（例えば、先頭からのバイト数）を与えて保存するようにしてもよい。

【0196】この保存処理と、上記した圧縮符号化処理および暗号化処理とは別々に行うようにしてもよい、同時に平行的に行うようにしてもよい。

【0197】さらに、ステップ S 22 において、録音プログラム 113 は、暗号化プログラム 137 に、予め定められている不揮発性メモリ 34 に記憶されている保存用鍵を使って、上述した DES 方式、FEAL 方式などの方式で、コンテンツを暗号化した暗号鍵を暗号化させ、HDD 21 の曲データベース（図 4 に示すコンテンツデータベース 114 の利用条件ファイル 162-1 乃至 162-N に対応する）に保存する。

【0198】ステップ S 23 において、録音プログラム 113 は、保存したファイルに関する情報、暗号化された暗号鍵、そのコンテンツの情報、使用者が GUI を介して入力した曲名の情報の要素を組にして HDD 21 の曲データベースに登録する（利用条件ファイル 162-1 乃至 162-N として記録する）。そして、ステップ S 2

4において、録音プログラム113は、CPU32に、曲データベース全体のハッシュ値を計算させ、不揮発性メモリ34に保存させる。

【0199】このようにして、例えば、図11に示するような曲データベースが、HDD21上に登録される。この例においては、アイテム1乃至アイテム3のファイル名、暗号化された暗号鍵、曲名、長さ、再生条件（開始日時、終了日時、回数制限）、再生回数カウンタ、再生時課金条件、コピー条件（回数）、コピー回数カウンタ、およびコピー条件（SCMS）が記録されている。

【0200】例えば、SDMI（Secure Digital Music Initiative）が規定する方式では、CDからコピーしたコンテンツに対応して、そのコンテンツがチェックアウトできる回数は、3回に設定される。

【0201】CDからHDD21にコンテンツが複製されて一定期間が経過すると、再びコンテンツを複製することができるようにしたので、ユーザの個人の使用の範囲とされる、数回の複製が可能となる。一方、個人の使用の範囲を超えて、例えば、大量に複製しようとする、莫大な時間が必要とされ、現実的に不可能になる。また、例えば、パーソナルコンピュータ1が故障して、HDD21に記録されていたコンテンツが消去された場合においても、一定期間の経過後、消去されたコンテンツを再び複製し、HDD21に記録することができる。

【0202】また、例えば、ネットワーク2を介してHDD21に記録されている期限データベースの内容を共有することもできる。

【0203】以上においては、ISRCに対応して複製された日時が記憶されている場合を例として説明したが、コンテンツやCDを識別する情報であれば、他のもの（例えば、曲名、アルバム名、それらの組み合わせなど）を利用することもできる。

【0204】次に、図12乃至図14のフローチャートを参照して、表示操作指示プログラム112およびコンテンツ管理プログラム111を実行するCPU11およびメインプログラムを実行するCPU52による、HDD21からポータブルデバイス6のフラッシュメモリ61（例えば、メモリスティック（商標））に、コンテンツを移動する処理およびチェックアウトの処理について説明する。

【0205】始めに、コンテンツの移動の処理について説明する。ステップS51において、移動管理プログラム134は、利用条件管理プログラム140に、曲データベース全体のハッシュ値を計算させ、ステップS52で、前回CPU32に計算させ、不揮発性メモリ34に保存しておいたハッシュ値と比較する。両者が一致しない場合、移動管理プログラム134は、ステップS53に進み、表示操作指示プログラム112に、例えば、「曲データベースが改竄された恐れがあります」のようなメッセージをディスプレイ20に表示させた後、処理を終

了させる。この場合の処理は、図8のステップS31乃至ステップS34の処理と同様の処理である。この場合においては、HDD21からポータブルデバイス6へのコンテンツの移動が実行されないことになる。

【0206】次に、ステップS54において、移動管理プログラム134は、HDD21に形成されている曲データベース（コンテンツデータベース114に含まれる）から、そこに登録されているコンテンツの情報を読み出し、表示操作指示プログラム112に、選択のためのGUIとしてディスプレイ20に表示させる。使用者は、この選択のためのGUIに基づいて、HDD21からポータブルデバイス6へ移動させるコンテンツを、図5のフィールド212に表示される曲名、ボタン216などをクリックして選択する。次に、ステップS55において、移動管理プログラム134は、ステップS54で選択された選択されたコンテンツの再生条件、コピー条件、再生時課金条件などを調べる。この処理の詳細は、図15のフローチャートを参照して後述する。

【0207】次に、ステップS56において、パーソナルコンピュータ1の認証プログラム141とポータブルデバイス6のCPU53との間において、相互認証処理が行われ、通信用鍵が共有される。

【0208】例えば、ポータブルデバイス6のフラッシュメモリ61（または、EEPROM68）には、マスター鍵KMMが予め記憶されており、パーソナルコンピュータ1のRAM13（または、HDD21の所定のファイル）には、個別鍵KPPとIDが予め記憶されているものとする。CPU53は、認証プログラム141から、RAM13に予め記憶されているIDの供給を受け、そのIDと自分自身が有するマスター鍵KMMにハッシュ関数を適用して、RAM13に記憶されているパーソナルコンピュータ1の個別鍵と同一の鍵を生成する。このようにすることで、パーソナルコンピュータ1とポータブルデバイス6の両方に、共通の個別鍵が共有されることになる。この個別鍵を用いてさらに、一時的な通信用鍵を生成することができる。

【0209】あるいはまた、パーソナルコンピュータ1のRAM13にIDとマスター鍵KMPを予め記憶させておくとともに、ポータブルデバイス6のフラッシュメモリ61にもポータブルデバイス6のIDと個別鍵KPMを記憶させておく。そして、それぞれのIDとマスター鍵をお互いに他方に送信することで、他方は一方から送信されてきたIDとマスター鍵にハッシュ関数を適用して、他方の個別鍵を生成する。そして、その個別鍵から、一時的な通信用鍵をさらに生成するようにする。

【0210】なお、認証の方法としては、例えば、IOS（International Organization for Standardization）9798-2を利用することができる。

【0211】相互認証が正しく行われなかったとき、処理は終了されるが、正しく行われたとき、さらに、ステップS57において、移動管理プログラム134は、コ

ンテンツデータベース 1 1 4 に、選択されたコンテンツのファイル名を曲データベースから読み出させ、そのファイル名のコンテンツ（例えば、図 7 のステップ S 2 0 の処理で暗号化されている）を HDD 2 1 から読み出す。ステップ S 5 8 において、移動管理プログラム 1 3 4 は、ステップ S 5 7 で読み出したデジタルデータであるコンテンツの圧縮符号化方式（ステップ S 1 9 の処理）、暗号化方式（ステップ S 2 0 の処理）、フォーマット（例えば、ヘッダの方式など）などをポータブルデバイス 6 のものに変換する処理を実行する。この変換処理の詳細は、図 1 7 のフローチャートを参照して後述する。

【0 2 1 2】ステップ S 5 9 において、移動管理プログラム 1 3 4 は、PD 用ドライバ 1 4 3 に、ステップ S 5 8 で変換したコンテンツを、USB ポート 2 3 を介してポータブルデバイス 6 に転送させる。ステップ S 6 0 において、ポータブルデバイス 6 の CPU 5 3 は、USB コネクタ 5 6 を介してこの伝送されてきたコンテンツを受信すると、そのコンテンツを、そのままフラッシュメモリ 6 1 に記憶させる。

【0 2 1 3】ステップ S 6 1 において、移動管理プログラム 1 3 4 は、さらに、利用条件変換プログラム 1 3 9 に、曲データベースに登録されているその選択されたコンテンツの再生条件（開始日時、終了日時、回数制限など）を、ポータブルデバイス 6 が管理している形式に変換する。ステップ S 6 2 において、移動管理プログラム 1 3 4 は、さらに、利用条件変換プログラム 1 3 9 に、選択されたコンテンツの曲データベース中に登録されているコピー条件中の SCMS 情報を、ポータブルデバイス 6 の管理する形式に変換させる。そして、ステップ S 6 3 において、移動管理プログラム 1 3 4 は、PD 用ドライバ 1 4 3 に、ステップ S 6 1 で変換した再生条件と、ステップ S 6 2 で変換した SCMS 情報を、ポータブルデバイス 6 に転送させる。ポータブルデバイス 6 の CPU 5 3 は、転送を受けた再生条件と SCMS 情報を、フラッシュメモリ 6 1 に保存する。

【0 2 1 4】ステップ S 6 4 において、移動管理プログラム 1 3 4 はまた、PD 用ドライバ 1 4 3 に、選択されたコンテンツの曲データベース中に登録されている再生条件、再生時課金条件、コピー条件などを、CPU 1 1 が曲データベース中で扱っている形式のまま、ポータブルデバイス 6 に転送させ、フラッシュメモリ 6 1 に保存させる。

【0 2 1 5】ステップ S 6 5 において、移動管理プログラム 1 3 4 は、コンテンツデータベース 1 1 4 に、選択されたコンテンツの暗号化されている暗号鍵を曲データベースから読み出させ、ステップ S 6 6 において、復号プログラム 1 4 2 に、その暗号鍵を RAM 1 3 に保存されている保存用鍵で復号させ、暗号化プログラム 1 3 7 に通信用鍵で暗号化させる。そして、通信用鍵で暗号化し

た暗号鍵を、移動管理プログラム 1 3 4 は、PD 用ドライバ 1 4 3 に、ポータブルデバイス 6 へ転送させる。

【0 2 1 6】ポータブルデバイス 6 の CPU 5 3 は、ステップ S 6 7 で、パーソナルコンピュータ 1 から転送されてきた暗号鍵を相互認証処理で共有した通信用鍵を用いて復号し、自分自身の保存用鍵を用いて暗号化し、既に保存したデータと関連付けて、フラッシュメモリ 6 1 に保存する。

【0 2 1 7】CPU 5 3 は、暗号鍵の保存が完了すると、ステップ S 6 8 において、パーソナルコンピュータ 1 に対して暗号鍵を保存したことを通知する。パーソナルコンピュータ 1 の移動管理プログラム 1 3 4 は、ポータブルデバイス 6 からこの通知を受けると、ステップ S 6 9 において、コンテンツデータベース 1 1 4 に、そのコンテンツに対応するコンテンツファイル 1 6 1 を削除させるとともに、曲データベースからそのコンテンツの要素の組（すなわち、利用条件ファイル 1 6 2）を削除させる。すなわち、これにより、コピーではなく、移動（ムーブ）が行われることになる。そして、ステップ S 7 0 において、移動管理プログラム 1 3 4 は、アダプタ 2 6 の CPU 3 2 に、曲データベースのデータを転送し、全体のハッシュ値を計算させ、不揮発性メモリ 3 4 に保存させる。このハッシュ値が、上述したステップ S 5 2 において、前回保存しておいたハッシュ値として用いられることになる。

【0 2 1 8】次に、パーソナルコンピュータ 1 からポータブルデバイス 6 にコンテンツをチェックアウトする処理について説明する。パーソナルコンピュータ 1 からポータブルデバイス 6 にコンテンツをチェックアウトする処理は、図 1 2 乃至図 1 4 のパーソナルコンピュータ 1 からポータブルデバイス 6 へコンテンツを移動させる場合と同様の処理である。すなわち、チェックアウトの処理は、パーソナルコンピュータ 1 においてチェックイン／チェックアウト管理プログラム 1 3 2 により実行され、図 1 4 のステップ S 6 9 において、コンテンツを削除する処理に代えて、曲データベースに登録されている、チェックアウトされたコンテンツのチェックアウトした回数（またはチェックアウトできる回数）を更新する処理を実行することを除いて、移動の場合の処理と基本的に同様の処理となるので、その処理の詳細の説明は省略する。

【0 2 1 9】次に、コンテンツ管理プログラム 1 1 1 を実行する CPU 1 1 による、図 1 2 のステップ S 5 5 における選択されたコンテンツの再生条件などのチェック処理について図 1 5 のフローチャートを参照して説明する。ステップ S 8 1 において、移動管理プログラム 1 3 4 は、コンテンツデータベース 1 1 4 に、曲データベースから、各種の条件を読み出させる。移動管理プログラム 1 3 4 は、ステップ S 8 2 において、ステップ S 8 1 で読み出した各種条件のうち、コピー回数がコピー制限

回数を既に過ぎているか否かを判定する。コピー回数が、コピー制限回数を既にすぎている場合には、それ以上コピーを許容する訳にはいかないので、ステップ S 8 3 に進み、移動管理プログラム 1 3 4 は、表示操作指示プログラム 1 1 2 に、例えば、「既にコピー回数がコピー制限回数に達しています」のようなメッセージをディスプレイ 2 0 に表示させ、処理を終了させる。ステップ S 8 2 において、コピー回数がコピー制限回数を過ぎていないと判定された場合、ステップ S 8 4 に進み、現在日時が再生終了日時を過ぎているか否かの判定が行われる。現在日時としては、アダプタ 2 6 の RTC 3 5 より出力されたものが用いられる。これにより、使用者が、パーソナルコンピュータ 1 の現在時刻を意図的に過去の値に修正したものが用いられるようなことが防止される。移動管理プログラム 1 3 4 は、この現在日時を CPU 3 2 から提供を受けて、ステップ S 8 4 の判断を自ら行うか、または、ステップ S 8 1 で、曲データベースから読み出した再生条件をアダプタ 2 6 の CPU 3 2 に供給し、CPU 3 2 に、ステップ S 8 4 の判定処理を実行させる。

【0220】現在日時が再生終了日時を過ぎている場合、ステップ S 8 5 に進み、移動管理プログラム 1 3 4 は、コンテンツデータベース 1 1 4 に、選択されたコンテンツを HDD 2 1 から消去させるとともに、曲データベースから、その選択されたコンテンツの情報を消去させる。ステップ S 8 6 において、移動管理プログラム 1 3 4 は、CPU 3 2 に、曲データベースのハッシュ値を計算させ、それを不揮発性メモリ 3 4 に保存させる。以後、処理は終了される。従って、この場合、コンテンツの移動が実行されない。

【0221】ステップ S 8 4 において、現在日時が、再生終了日時を過ぎていないと判定された場合、ステップ S 8 7 に進み、移動管理プログラム 1 3 4 は、その選択されたコンテンツの再生時課金条件（例えば、再生 1 回当たりの料金）が曲データベース中に登録されているか否かを判定する。再生時課金条件が登録されている場合には、移動管理プログラム 1 3 4 は、ステップ S 8 8 において、PD 用ドライバ 1 4 3 に、ポータブルデバイス 6 と通信させ、ポータブルデバイス 6 に課金機能が存在するか否かを判定する。ポータブルデバイス 6 に課金機能が存在しない場合には、選択されたコンテンツをポータブルデバイス 6 に転送する訳にはいかないので、ステップ S 8 9 において、移動管理プログラム 1 3 4 は、表示操作指示プログラム 1 1 2 に、例えば、「転送先が課金機能を有していません」のようなメッセージをディスプレイ 2 0 に表示させ、コンテンツの移動処理を終了させる。

【0222】ステップ S 8 7 において再生時課金条件が登録されていないと判定された場合、または、ステップ S 8 8 において、ポータブルデバイス 6 に課金機能が存在すると判定された場合、ステップ S 9 0 に進み、移動

管理プログラム 1 3 4 は、選択されたコンテンツに関し、例えば、再生制限回数などのその他の再生条件が登録されているか否かを判定する。その他の再生条件が登録されている場合には、ステップ S 9 1 に進み、移動管理プログラム 1 3 4 は、ポータブルデバイス 6 に、その再生条件を守る機能が存在するか否かを判定する。ポータブルデバイス 6 が、その再生条件を守る機能を有していない場合には、ステップ S 9 2 に進み、移動管理プログラム 1 3 4 は、表示操作指示プログラム 1 1 2 に、例えば、「転送先の装置が再生条件を守る機能を有していません」のようなメッセージをディスプレイ 2 0 に表示させ、処理を終了させる。

【0223】ステップ S 9 0 において、再生条件が登録されていないと判定された場合、またはステップ S 9 1 において、ポータブルデバイス 6 が再生条件を守る機能を有していると判定された場合、再生条件等のチェック処理が終了され、図 1 2 のステップ S 5 6 に戻る。

【0224】図 1 6 は、ポータブルデバイス 6 が管理している（守ることが可能な）再生条件の例を表している。図 1 6 に示す再生情報は、例えば、EEPROM 6 8 に記憶されている。この例においては、アイテム 1 乃至アイテム 3 の各コンテンツについて、再生開始日時と再生終了日時が登録されているが、再生回数は、アイテム 2 についてのみ登録されており、アイテム 1 とアイテム 3 については登録されていない。従って、アイテム 2 のコンテンツが選択されたコンテンツとされた場合、再生回数の再生条件は守ることが可能であるが、アイテム 1 またはアイテム 3 のコンテンツが選択されたコンテンツとされた場合、再生回数の条件は守ることができないことになる。

【0225】次に、図 1 7 のフローチャートを参照して、コンテンツ管理プログラム 1 1 1 を実行する CPU 1 1 による、図 1 2 のステップ S 5 8 におけるフォーマット変換処理の詳細について説明する。ステップ S 1 0 1 において、移動管理プログラム 1 3 4 は、コンテンツデータベース 1 1 4 に記録されている選択されたコンテンツのフォーマット（例えば、再生条件、使用条件、コピー条件などを含むヘッダなどの方式）を調べる。ステップ S 1 0 2 において、移動管理プログラム 1 3 4 は、相手先の機器（今の場合、ポータブルデバイス 6）に設定することが可能な条件を調べる。すなわち、移動管理プログラム 1 3 4 は、ポータブルデバイス 6 の CPU 5 3 に設定可能な条件を問い合わせ、その回答を得る。ステップ S 1 0 3 において移動管理プログラム 1 3 4 は、曲データベース中に登録されているフォーマットの条件のうち、相手先の機器に設定可能な条件をステップ S 1 0 2 で調べた条件に基づいて決定する。

【0226】ステップ S 1 0 4 において、移動管理プログラム 1 3 4 は、設定可能な条件が存在するか否かを判定し、設定可能な条件が存在しない場合には、ステップ

S 105に進み、コンテンツをポータブルデバイス6に移動する処理を禁止する。すなわち、この場合には、曲データベース中に登録されている条件をポータブルデバイス6が守ることができないので、そのようなポータブルデバイス6には、コンテンツを移動することが禁止されるのである。

【0227】ステップS104において設定可能な条件が存在すると判定された場合、ステップS106に進み、移動管理プログラム134は、利用条件変換プログラム139に、その条件を相手先の機能フォーマットの条件（例えば、ポータブルデバイス6に転送する際、ヘッダに格納される条件）に変換させる。そして、ステップS107において、移動管理プログラム134は、変換した条件を相手先の機器に設定する。その結果、ポータブルデバイス6は、設定された条件に従って（その条件を守って）、コンテンツを再生することが可能となる。

【0228】次に、図18乃至図20のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11およびメインプログラムを実行するCPU53による、HDD21からポータブルデバイス6にコンテンツをコピーする場合の処理について説明する。この図18乃至図20のステップS111乃至ステップS127の処理は、コピー管理プログラム133により実行され、図12乃至図14のHDD21からポータブルデバイス6へコンテンツを移動させる場合のステップS51乃至ステップS67の処理と同様の処理である。すなわち、この場合においても、曲データベースの改竄がチェックされた後、選択されたコンテンツの再生条件とのチェック処理が行われる。さらに、ポータブルデバイス6と、パーソナルコンピュータ1との間の相互認証処理の後、コンテンツが、パーソナルコンピュータ1のHDD21からポータブルデバイス6のフラッシュメモリ61に転送され、保存される。その後、ステップS128において、コピー管理プログラム133は、曲データベースのコピー回数カウンタを1だけインクリメントする。そして、ステップS129において、コピー管理プログラム133は、CPU32に、曲データベース全体のハッシュ値を計算させ、その値を不揮発性メモリ34に保存させる。

【0229】次に、図21のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11およびメインプログラムを実行するCPU53による、ポータブルデバイス6からHDD21にコンテンツを移動する処理およびチェックインの処理について説明する。

【0230】始めに、コンテンツの移動の処理について説明する。ステップS161において、移動管理プログラム134は、ポータブルデバイス6のCPU53に対してフラッシュメモリ61に記憶されているコンテンツの情報の読み出しを要求する。CPU53は、この要求に対応して、フラッシュメモリ61に記憶されているコンテ

ンツの情報をパーソナルコンピュータ1に送信する。移動管理プログラム134は、この情報に基づいて、ディスプレイ20に、フラッシュメモリ61に記憶されているコンテンツを選択するためのGUIを表示させる。使用者は、キーボード18またはマウス19を操作して、そのGUIに基づいて、ポータブルデバイス6からHDD21（コンテンツデータベース114）に移動させるコンテンツを指定する。

【0231】ステップS162において、移動管理プログラム134は、認証プログラム141に、CPU53との間において、相互認証処理を実行させ、通信用鍵を共有させる。この処理は、図12のステップS56における場合と同様の処理である。

【0232】次に、ステップS163において、CPU53は、フラッシュメモリ61に記憶されている暗号化されている選択されたコンテンツを読み出し、パーソナルコンピュータ1に転送する。移動管理プログラム134は、ステップS164において、ポータブルデバイス6から転送されてきたコンテンツを、1つのファイルとしてファイル名を付けて、コンテンツデータベース114（HDD21）に保存する。この保存は、例えば、1つのファイルの一部として、ファイル名の位置情報（例えば、先頭からのバイト数）を与えて行うようにすることもできる。

【0233】ステップS165において、CPU53は、フラッシュメモリ61に記憶されている選択されたコンテンツの暗号化されている暗号鍵を読み出し、それを自分自身の保存用鍵で復号し、さらに通信用鍵で暗号化した後、パーソナルコンピュータ1に転送する。この暗号鍵は、例えば、図14のステップS67の処理でフラッシュメモリ61に保存されていたものである。

【0234】ステップS166において、移動管理プログラム134は、ポータブルデバイス6から暗号鍵の転送を受けると、復号プログラム142に、それを通信用鍵で復号させ、暗号化プログラム137に、自分自身の保存用鍵で暗号化させる。ステップS167で、移動管理プログラム134は、コンテンツデータベース114に、ステップS164で保存したコンテンツのファイル名、そのコンテンツの情報、使用者がGUIを介して入力した曲名、ステップS166で暗号化した暗号鍵などを、HDD21の曲データベースに登録させる。そして、ステップS168において、移動管理プログラム134は、利用条件管理プログラム140に、その曲データベース全体のハッシュ値をCPU32に計算させ、不揮発性メモリ34に保存させる。

【0235】ステップS169において、移動管理プログラム134は、ポータブルデバイス6に対して暗号鍵が保存されたことを通知し、そのコンテンツの削除を要求する。CPU53は、パーソナルコンピュータ1から、そのコンテンツの削除が要求されてきたとき、ステップ

S 1 7 0において、フラッシュメモリ 6 1に記憶されているそのコンテンツを削除する。

【0236】次に、ポータブルデバイス 6からパーソナルコンピュータ 1にコンテンツをチェックインする処理について説明する。ポータブルデバイス 6からパーソナルコンピュータ 1にコンテンツをチェックインする処理は、図 2 1のポータブルデバイス 6からパーソナルコンピュータ 1へコンテンツを移動させる場合と同様の処理である。すなわち、チェックインの処理は、パーソナルコンピュータ 1においてチェックイン／チェックアウト 10 管理プログラム 1 3 2により実行され、図 2 1のステップ S 1 6 2乃至 S 1 6 6の処理が省略される。また、パーソナルコンピュータ 1は、図 2 1のステップ S 1 6 7において、曲データベースに記録されている、チェックインされたコンテンツのチェックアウトできる回数を更新する処理を実行して、ステップ S 1 7 0の処理の後、コンテンツファイルの削除を確認することを除いて、移動の場合の処理と基本的に同様の処理となるので、その処理の詳細の説明は省略する。

【0237】なお、ポータブルデバイス 6のフラッシュメモリ 6 1がメモリカードとして着脱可能であるとき、パーソナルコンピュータ 1は、チェックインの処理において、図 2 1のステップ S 1 6 2の相互認証の処理を実行する。

【0238】また、前述のように、所定のパーソナルコンピュータからチェックアウトされたコンテンツが、該パーソナルコンピュータにのみチェックインできるようになっており、チェックイン処理の前処理として、選択されたコンテンツが、チェックインを行う PCからチェックアウトされたかを判断し、該 PCからチェックアウトされたものではないと判断されたらば、チェックインを行わないように処理するステップが存在する。例えば、図 5のフィールド 2 1 3の×がついたコンテンツをチェックインしようとした場合がそれにあたる。

【0239】次に、コンテンツ管理プログラム 1 1 1を実行する CPU 1 1およびメインプログラムを実行する CPU 5 3による、ポータブルデバイス 6から HDD 2 1へコンテンツをコピーする場合の処理について、図 2 2のフローチャートを参照して説明する。この図 2 2に示すステップ S 1 8 1乃至ステップ S 1 8 8の処理は、図 2 1のポータブルデバイス 6から HDD 2 1へコンテンツを移動させる場合の処理におけるステップ S 1 6 1乃至ステップ S 1 6 8の処理と同様の処理である。すなわち、コピー処理の場合は、コピー管理プログラム 1 3 3により実行され、図 2 1のステップ S 1 6 9、S 1 7 0の処理が省略される点を除いて、移動の場合の処理と基本的に同様の処理となるので、その説明は省略する。

【0240】次に、図 2 3のフローチャートを参照して、EMDサーバ 4およびコンテンツ管理プログラム 1 1 1を実行する CPU 1 1による、EMDサーバ 4から転送を受

けたコンテンツを HDD 2 1にコピーする処理について説明する。ステップ S 2 0 1において、購入用プログラム 1 4 4は、図 5に示すボタン 2 0 2がクリックされて、使用者から EMDサーバ 4へのアクセスが指令されたとき、通信部 2 5を制御し、ネットワーク 2を介して EMDサーバ 4にアクセスさせる。EMDサーバ 4は、このアクセスに対応して、自分自身が保持しているコンテンツの曲番号、曲名、各情報などの情報を、ネットワーク 2を介してパーソナルコンピュータ 1に転送する。購入用プログラム 1 4 4は、通信部 2 5を介して、この情報を取得したとき、表示操作指示プログラム 1 1 2に、それをインタフェース 1 7を介してディスプレイ 2 0に表示させる。使用者は、ディスプレイ 2 0に表示された GUIを利用して、ステップ S 2 0 2において、コピーを希望するコンテンツを指定する。この指定情報は、ネットワーク 2を介して EMDサーバ 4に転送される。ステップ S 2 0 3において、購入用プログラム 1 4 4は、EMDサーバ 4との間において、ネットワーク 2を介して相互認証処理を実行し、通信用鍵を共有する。

【0241】パーソナルコンピュータ 1と EMDサーバ 4との間で行われる相互認証処理は、例えば、ISO 9 7 9 8-3で規定される公開鍵と秘密鍵を用いて行うようにすることができる。この場合、パーソナルコンピュータ 1は、自分自身の秘密鍵と EMDサーバ 4の公開鍵を予め有しており、EMDサーバ 4は、自分自身の秘密鍵を有し、相互認証処理が行われる。パーソナルコンピュータ 1の公開鍵は、EMDサーバ 4から転送したり、あるいはパーソナルコンピュータ 1に予め配布されている証明書 (certificate) をパーソナルコンピュータ 1から EMDサーバ 4に転送し、その証明書を EMDサーバ 4が確認し、公開鍵を得るようにしてもよい。さらに、ステップ S 2 0 4において、購入用プログラム 1 4 4は、EMDサーバ 4との間において課金に関する処理を実行する。この課金の処理の詳細は、図 2 4のフローチャートを参照して後述する。

【0242】次に、ステップ S 2 0 5において、EMDサーバ 4は、パーソナルコンピュータ 1に対して、ステップ S 2 0 2で指定された、暗号化されているコンテンツをネットワーク 2を介してパーソナルコンピュータ 1に転送する。このとき、時刻情報も適宜転送される。ステップ S 2 0 6において、購入用プログラム 1 4 4は、コンテンツデータベース 1 1 4に、転送を受けたコンテンツにファイル名を付けて HDD 2 1に 1つのコンテンツファイル 1 6 1として保存させる。ステップ S 2 0 7において、EMDサーバ 4は、さらに、そのコンテンツの暗号鍵をステップ S 2 0 3でパーソナルコンピュータ 1と共有した通信用鍵を用いて暗号化し、パーソナルコンピュータ 1へ転送する。

【0243】購入用プログラム 1 4 4は、ステップ S 2 0 8において、復号プログラム 1 4 2に、EMDサーバ 4

より転送を受けた暗号鍵を単独で、またはアダプタ 26 の CPU 32 と共同して通信用鍵を用いて復号させ、暗号化プログラム 137 に、復号して得られた暗号鍵を自分自身の保存用鍵で暗号化させる。ステップ S 209 において、購入用プログラム 144 は、コンテンツデータベース 114 に、そのコンテンツのファイル名、コンテンツの情報、使用者が入力した曲名、暗号化された暗号鍵を組にして、HDD 21 の曲データベースに登録させる。さらに、ステップ S 210 において、購入用プログラム 144 は、その曲データベース全体のハッシュ値を CPU 32 に計算させ、不揮発性メモリ 34 に保存させる。

【0244】なお、ステップ S 205 において EMD サーバ 4 は、コンテンツとともに、時刻データをパーソナルコンピュータ 1 に送信する。この時刻データは、パーソナルコンピュータ 1 からアダプタ 26 に転送される。アダプタ 26 の CPU 32 は、パーソナルコンピュータ 1 より転送されてきた時刻データを受信すると、ステップ S 211 において、RTC 35 の時刻を修正させる。このようにして、相互認証の結果、正しい装置と認識された外部の装置から得られた時刻情報に基づいて、アダプタ 26 の RTC 35 の時刻情報を修正するようにしたので、アダプタ 26 を常に正しい時刻情報を保持することが可能となる。

【0245】次に、図 24 のフローチャートを参照して、EMD サーバ 4 およびコンテンツ管理プログラム 111 を実行する CPU 11 による、図 23 のステップ S 204 における課金に関する処理の詳細について説明する。ステップ S 221 において、購入用プログラム 144 は、ステップ S 201 で EMD サーバ 4 から伝送されてきた価格情報の中から、ステップ S 202 で指定された選択されたコンテンツの価格情報を読み取り、これを HDD 21 上の課金ログに書き込む。図 25 は、このような課金ログの例を表している。この例においては、使用者は、アイテム 1 乃至アイテム 3 を、EMD サーバ 4 からコピーしており、アイテム 1 とアイテム 2 の領域は 50 円とされ、アイテム 3 の料金は 60 円とされている。その時点における課金ログのハッシュ値も、CPU 32 により計算され、不揮発性メモリ 34 に登録されている。

【0246】次に、ステップ S 222 において、購入用プログラム 144 は、ステップ S 221 で書き込んだ課金ログを HDD 21 から読み出し、これをネットワーク 2 を介して EMD サーバ 4 に転送する。EMD サーバ 4 は、ステップ S 223 において、パーソナルコンピュータ 1 から転送を受けた課金ログに基づく課金計算処理を実行する。すなわち、EMD サーバ 4 は、内蔵するデータベースに、パーソナルコンピュータ 1 の使用者から伝送されてきた課金ログを追加更新する。そして、ステップ S 224 において、EMD サーバ 4 は、その課金ログについて直ちに決裁するか否かを判定し、直ちに決裁する場合には、ステップ S 225 に進み、EMD サーバ 4 は、決裁に

必要な商品名、金額などを決裁サーバ（図示せず）に転送する。そして、ステップ S 226 において、決裁サーバは、パーソナルコンピュータ 1 の使用者に対する決裁処理を実行する。ステップ S 224 において、決裁は直ちには行われないと判定された場合、ステップ S 225 と S 226 の処理はスキップされる。すなわち、この処理は、例えば、月に 1 回など、定期的にその後実行される。

【0247】次に、図 26 と図 27 のフローチャートを参照して、コンテンツ管理プログラム 111 を実行する CPU 11 による、音声入出力インタフェース 24 の IEC60958 端子 24a から入力された、図示せぬ CD プレーヤなどからの再生されたコンテンツを、HDD 21 にコピーする場合の処理について説明する。ステップ S 241 において、使用者は、CD プレーヤの IEC60958 出力端子を、パーソナルコンピュータ 1 の音声入出力インタフェース 24 の IEC60958 端子 24a に接続する。ステップ S 242 において、使用者は、キーボード 18 またはマウス 19 を操作し、CD プレーヤからコピーするコンテンツの曲名（または、コンテンツに対応する番号）を入力する。そして、ステップ S 243 において使用者は、CD プレーヤのボタンを操作し、CD プレーヤの再生を開始させる。CD プレーヤとパーソナルコンピュータ 1 との間に制御信号を送受する線が接続されている場合には、パーソナルコンピュータ 1 のキーボード 18 またはマウス 19 を介して再生開始指令を入力することで、CD プレーヤに CD の再生を開始させることも可能である。

【0248】CD プレーヤにおいて、CD の再生が開始されると、ステップ S 244 において、CD プレーヤから出力されたコンテンツが、IEC60958 端子 24a を介してパーソナルコンピュータ 1 に転送されてくる。ステップ S 245 において、コピー管理プログラム 133 は、IEC60958 端子 24a を介して入力されてくるデータから、SCMS (Serial Copy Management System) データを読み取る。この SCMS データには、コピー禁止、コピー 1 回限り可能、コピーフリーなどのコピー情報が含まれている。そこで、ステップ S 246 において、CPU 11 は、SCMS データがコピー禁止を表しているか否かを判定し、コピー禁止を表している場合には、ステップ S 247 に進み、コピー管理プログラム 133 は、表示操作指示プログラム 112 に、例えば、「コピーが禁止されています」といったメッセージをディスプレイ 20 に表示させ、コピー処理を終了する。すなわち、この場合には、HDD 21 へのコピーが禁止される。

【0249】コピー管理プログラム 133 は、ステップ S 246 において、ステップ S 245 で読み取った SCMS 情報がコピー禁止を表していないと判定した場合、ステップ S 248 に進み、ウォータマークコードを読み出し、そのウォータマークがコピー禁止を表しているか否かをステップ S 249 において判定する。ウォータマー

クコードがコピー禁止を表している場合には、ステップ S 2 4 7 に進み、上述した場合と同様に、所定のメッセージが表示され、コピー処理が終了される。

【0250】ステップ S 2 4 9 において、ウォータマークがコピー禁止を表していないと判定された場合、ステップ S 2 5 0 に進み、期限データベースチェック処理が行われる。期限データベースチェックの結果、選択されたコンテンツが既に登録されていれば、ステップ S 2 5 1、S 2 5 2 の処理で、処理が終了される。この処理は、図 7 のステップ S 1 3、S 1 4 の処理と同様の処理である。

【0251】選択されたコンテンツがまだ HDD 2 1 に登録されていないコンテンツであれば、ステップ S 2 5 3 乃至 S 2 5 8 で、その登録処理が実行される。このステップ S 2 5 3 乃至ステップ S 2 5 8 の処理は、ステップ S 2 5 7 において、IEC60958 端子 2 4 a から供給されてくる SCMS 情報も曲データベースに登録される点を除き、図 7 のステップ S 1 9 乃至ステップ S 2 4 の処理と同様の処理であるので、その説明は省略する。

【0252】次に、図 2 8 と図 2 9 のフローチャートを参照して、コンテンツ管理プログラム 1 1 1 を実行する CPU 1 1 による、コンテンツを HDD 2 1 から IEC60958 端子 2 4 a へ出力（再生）する場合の処理について説明する。ステップ S 2 7 1 乃至ステップ S 2 7 3 において、図 1 8 のステップ S 1 1 1 乃至 S 1 1 3 における場合と同様に、曲データベース全体のハッシュ値が計算され、前回保存しておいたハッシュ値と一致するかが判定され、曲データベースの改竄のチェック処理が行われる。曲データベースの改竄が行われていないと判定された場合、ステップ S 2 7 4 に進み、表示操作指示プログラム 1 1 2 は、コンテンツ管理プログラム 1 1 1 を介して、コンテンツデータベース 1 1 4 に、HDD 2 1 の曲データベースにアクセスさせ、そこに登録されている曲の情報を読み出させ、ディスプレイ 2 0 に表示させる。使用者は、その表示を見て、キーボード 1 8 またはマウス 1 9 を適宜操作して、再生出力するコンテンツを選択する。ステップ S 2 7 5 において、表示操作指示プログラム 1 1 2 は、選択されたコンテンツの再生条件等のチェック処理を実行する。この再生条件等のチェック処理の詳細は、図 3 0 のフローチャートを参照して後述する。

【0253】次に、ステップ S 2 7 6 において、表示操作指示プログラム 1 1 2 は、コンテンツ管理プログラム 1 1 1 を介して、コンテンツデータベース 1 1 4 に、ステップ S 2 7 4 において選択されたコンテンツの暗号鍵を曲データベースから読み出させ、復号プログラム 1 4 2 に保存用鍵で復号させる。ステップ S 2 7 7 において、表示操作指示プログラム 1 1 2 は、コンテンツ管理プログラム 1 1 1 を介して、コンテンツデータベース 1 1 4 に、選択されたコンテンツの SCMS 情報を曲データベースから読み出させ、IEC60958 端子 2 4 a から出力する

SCMS 情報を、SCMS システムの規則に従って決定する。例えば、再生回数に制限があるような場合、再生回数は 1 だけインクリメントされ、新たな SCMS 情報とされる。ステップ S 2 7 8 において、表示操作指示プログラム 1 1 2 はさらに、コンテンツ管理プログラム 1 1 1 を介して、コンテンツデータベース 1 1 4 に、選択されたコンテンツの ISRC を曲データベースから読み出させる。

【0254】次に、ステップ S 2 7 9 において、表示操作指示プログラム 1 1 2 は、コンテンツ管理プログラム 1 1 1 を介して、コンテンツデータベース 1 1 4 に、曲データベースから選択されたコンテンツファイル名を読み出させ、そのファイル名を基に、そのコンテンツを HDD 2 1 から読み出させる。表示操作指示プログラム 1 1 2 はさらに、コンテンツ管理プログラム 1 1 1 を介して、コンテンツデータベース 1 1 4 に、そのコンテンツに対応する暗号鍵を曲データベースから読み出させ、復号プログラム 1 4 2 に、保存用鍵で復号させ、復号した暗号鍵を用いて、暗号化されているコンテンツを復号する。圧縮／伸張プログラム 1 3 8 は、さらに、そのコンテンツの圧縮符号を復号（伸張）する。ステップ S 2 8 0 において、表示操作指示プログラム 1 1 2 は、ドライバ 1 1 7 に、ステップ S 2 7 9 で、復号したデジタルデータであるコンテンツを、ステップ S 2 7 7 で決定した SCMS 情報、並びにステップ S 2 7 8 で読み出した ISRC 情報とともに、IEC60958 の規定に従って、IEC60958 端子 2 4 a から出力させる。さらにまた、表示操作指示プログラム 1 1 2 は、例えば、図示せぬリアルプレーヤ（商標）などのプログラムを動作させ、デジタルデータであるコンテンツをアナログ化させ、音声入出力インタフェース 2 4 のアナログ出力端子から出力させる。

【0255】ステップ S 2 8 1 において、表示操作指示プログラム 1 1 2 は、コンテンツ管理プログラム 1 1 1 を介して、コンテンツデータベース 1 1 4 に、曲データベース中の再生回数カウンタの値を 1 だけインクリメントさせる。そして、ステップ S 2 8 2 において、選択されたコンテンツに再生時課金条件が付加されているかを判定する。再生時課金条件が付加されている場合には、ステップ S 2 8 3 に進み、表示操作指示プログラム 1 1 2 は、コンテンツ管理プログラム 1 1 1 を介して、コンテンツデータベース 1 1 4 に、対応する料金を課金ログに書き込ませ、ステップ S 2 8 4 において、表示操作指示プログラム 1 1 2 は、利用条件管理プログラム 1 4 0 に、曲データベース全体のハッシュ値を CPU 3 2 に計算させ、不揮発性メモリ 3 4 に記憶させる。ステップ S 2 8 2 において、選択されたコンテンツに再生時課金条件が付加されていないと判定された場合、ステップ S 2 8 3 とステップ S 2 8 4 の処理はスキップされる。

【0256】次に、図 3 0 のフローチャートを参照して、コンテンツ管理プログラム 1 1 1 を実行する CPU 1 1 による、図 2 8 のステップ S 2 7 5 の再生条件等のチ

チェック処理の詳細について説明する。ステップS301において、表示操作指示プログラム112は、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、曲データベースの各種条件を読み出させる。ステップS302において利用条件管理プログラム140は、読み出した条件のうち、再生回数が制限回数を過ぎているか否かを判定し、過ぎている場合には、ステップS303に進み、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、選択されたコンテンツをHDD21から削除させるとともに、曲データベースから選択されたコンテンツの情報を削除させる。ステップS304において、表示操作指示プログラム112はさらに、利用条件管理プログラム140に、曲データベースの新たなハッシュ値をCPU32に計算させ、そのハッシュ値を不揮発性メモリ34に保存させる。この場合、再生出力は禁止される。

【0257】ステップS302において、再生回数が制限回数を過ぎていないと判定された場合、ステップS305に進み、利用条件管理プログラム1402は、再生終了日時が現在日時を過ぎているか否かを判定する。再生終了日時が現在日時を過ぎている場合には、上述した場合と同様にステップS303において、選択されたコンテンツをHDD21から削除させるとともに、曲データベースからも削除させる。そして、ステップS304において、新たな曲データベースのハッシュ値が計算され、保存される。この場合にも、再生出力は禁止される。

【0258】ステップS305において、再生終了日時が現在日時を過ぎていると判定された場合は、ステップS306に進み、CPU32は、その選択されたコンテンツに対して再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップS307に進み、表示操作指示プログラム112は、再生時課金条件が付加されている旨のメッセージと料金を、ディスプレイ20に表示させる。ステップS306において、再生時課金条件が付加されていないと判定された場合、ステップS307の処理はスキップされる。

【0259】次に、図31と図32のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11およびメインプログラムを実行するCPU53による、HDD21からポータブルデバイス6経由でコンテンツを出力（再生）する場合の処理について説明する。ステップS321乃至ステップS325において、曲データベースの改竄チェックと選択されたコンテンツの指定、並びに選択されたコンテンツの再生条件等のチェック処理が行われる。その処理は、図28のステップS271乃至ステップS275の処理と同様の処理であるので、その説明は省略する。

【0260】ステップS326において、ポータブルデ

バイス6とパーソナルコンピュータ1の間で相互認証処理が実行され、相互の間で、通信用鍵が共有される。ステップS327において、表示操作指示プログラム112は、ポータブルデバイス6に対して、これから送る暗号化されているコンテンツを再生するように命令する。ステップS328において、表示操作指示プログラム112は、ステップS324で、コンテンツ管理プログラム111を介してコンテンツデータベース114に、指定された選択されたコンテンツのファイル名を曲データベースから読み出させ、そのファイル名のコンテンツをHDD21から読み出させる。表示操作指示プログラム112は、ステップS329において、コンテンツ管理プログラム111に、コンテンツの圧縮符号化方式、暗号化方式、フォーマットなどをポータブルデバイス6の方式のものに変換する処理を実行させる。そして、ステップS330において、表示操作指示プログラム112は、暗号化プログラム137に、ステップS329において変換したコンテンツを通信用鍵で暗号化させ、ポータブルデバイス6に転送する。

【0261】ステップS331において、ポータブルデバイス6のCPU53は、ステップS327において、パーソナルコンピュータ1から転送されてきた命令に対応して、転送を受けた各データを通信用鍵で復号し、再生出力する。ステップS332において、表示操作指示プログラム112は、コンテンツ管理プログラム111を介してコンテンツデータベース114に、曲データベースの再生回数カウントを1だけインクリメントさせる。さらに、ステップS333において、表示操作指示プログラム112は、選択されたコンテンツに再生時課金条件が付加されているか否かを判定し、付加されている場合には、ステップS334において、コンテンツ管理プログラム111を介してコンテンツデータベース114に、その料金を課金ログに書き込ませ、ステップS335において、CPU32に、曲データベース全体のハッシュ値を新たに計算させ、保存させる。選択されたコンテンツに再生時課金条件が付加されていない場合には、ステップS334、ステップS335の処理はスキップされる。

【0262】本発明においては、コンテンツが不正に複製されるのを防止するために、各種の工夫が凝らされている。例えば、CPU11を動作させるプログラムは、その実行順序が毎回変化するような、いわゆるタンパレジスタントソフトウェアとされている。

【0263】さらに、上述したように、CPU11の機能の一部は、ハードウェアとしてのアダプタ26に分担され、両者が共働して各種の処理を実行するようになされている。これにより、より安全性を高めることが可能となっている。

【0264】例えば、上述したように、曲データベースのハッシュ値は、曲データベース自体に保存されるので

はなく、アダプタ 2 6 の不揮発性メモリ 3 4 に保存される。すなわち、図 8 のステップ S 3 2, S 3 3 などの前回保存しておいたハッシュ値との比較処理において、比較対象とされる過去のハッシュ値は、不揮発性メモリ 3 4 に記憶されているものとされる。これにより、例えば、他の記録媒体にコピーまたは移動させる前に、HDD 2 1 に保存されているコンテンツを含む記録内容の全てをバックアップしておき、HDD 2 1 から、そこに保存されているコンテンツを他の記録媒体にコピーまたは移動した後、HDD 2 1 にバックアップしておいた記録内容に 10 含まれるコンテンツを再びリストアするようにすることで、利用条件を無視して、実質的に際限なく、コピーまたは移動ができてしまうことが防止される。

【0 2 6 5】例えば、図 3 3 に示すように、HDD 2 1 にコンテンツ A, B が保存されている場合、不揮発性メモリ 3 4 には、コンテンツ A とコンテンツ B の情報に対応するハッシュ値が保存されている。この状態において、HDD 2 1 のコンテンツ A, B を含む記録データの一部または全部を他の記録媒体 2 7 1 にバックアップしたとする。その後、HDD 2 1 に保存されているコンテンツ A と 20 コンテンツ B のうち、コンテンツ A を他の記録媒体 2 7 2 に移動させた場合、その時点において、HDD 2 1 に記録されているコンテンツは、コンテンツ B だけとなるので、不揮発性メモリ 3 4 のハッシュ値も、コンテンツ B に対応するハッシュ値に変更される。

【0 2 6 6】従って、その後、記録媒体 2 7 1 にバックアップしておいた HDD 2 1 のコンテンツ A, B を含む記録データの一部または全部を HDD 2 1 にリストアして、HDD 2 1 に、再びコンテンツ A とコンテンツ B を保存させたとしても、不揮発性メモリ 3 4 には、コンテンツ B の 30 情報から演算されたハッシュ値が記憶されており、コンテンツ A とコンテンツ B の情報から演算されたハッシュ値は記憶されていない。これにより、その時点において、HDD 2 1 に記憶されているコンテンツ A とコンテンツ B に基づくハッシュ値が、不揮発性メモリ 3 4 に記憶されている過去のハッシュ値と一致しないことになり、曲データベースが改竄されたことが検出される。その結果、以後、HDD 2 1 に保存されているコンテンツ A とコンテンツ B の利用が制限されてしまうことになる。

【0 2 6 7】さらに、上述したように、アダプタ 2 6 は、RTC 3 5 を内蔵しており、この RTC 3 5 の値は、正しい認証結果が得られた他の装置（例えば、EMD サーバ 4）から転送されてきた時刻データに基づいて、その時刻情報を修正する。そして、現在日時としては、パーソナルコンピュータ 1 が管理するものではなく、RTC 3 5 が出力するものが利用される。従って、使用者が、パーソナルコンピュータ 1 の現在時刻を故意に過去の時刻に修正し、再生条件としての再生終了日時の判定を免れるようなことができなくなる。

【0 2 6 8】また、アダプタ 2 6 は、暗号化されて転送 50

されてきたプログラムを ROM 3 6 に予め記憶されているプログラムに従って復号し、実行するように構成することで、より安全性が高められている。次に、この点について、図 3 4 のフローチャートを参照して説明する。

【0 2 6 9】すなわち、パーソナルコンピュータ 1 は、アダプタ 2 6 に対して、所定の処理を実行させたいとき、ステップ S 3 5 1 において、アダプタ 2 6 に実行させるべきプログラムを RAM 1 3 に予め記憶されている暗号鍵を用いて暗号化してアダプタ 2 6 に転送する。アダプタ 2 6 の ROM 3 6 には、パーソナルコンピュータ 1 から転送されてきた、暗号化されているプログラムを復号し、実行するためのプログラムが予め記憶されている。CPU 3 2 は、この ROM 3 6 に記憶されているプログラムに従って、パーソナルコンピュータ 1 から転送されてきた暗号化されているプログラムをステップ S 3 5 2 において復号する。そして、ステップ S 3 1 3 において、CPU 3 2 は、復号したプログラムを RAM 3 3 に展開し、ステップ S 3 5 4 において、そのプログラムを実行する。

【0 2 7 0】例えば、上述したように、パーソナルコンピュータ 1 の CPU 1 1 は、HDD 2 1 の曲データベースのハッシュ値をアダプタ 2 6 に計算させるとき、曲データベースのデータを暗号鍵で暗号化してアダプタ 2 6 の CPU 3 2 に転送する。CPU 3 2 は、転送されてきた曲データベースのデータに対してハッシュ関数を適応し、ハッシュ値を計算する。そして、計算されたハッシュ値を不揮発性メモリ 3 4 に記憶させる。あるいは、そのハッシュ値を、CPU 3 2 は、予め記憶されている過去のハッシュ値と比較し、比較結果をパーソナルコンピュータ 1 の CPU 1 1 に転送する。

【0 2 7 1】図 3 5 は、アダプタ 2 6 の内部のより具体的な構成を表している。アダプタ 2 6 は、半導体 IC として形成される。アダプタ 2 6 は、図 2 に示したインタフェース 3 1、CPU 3 2、RAM 3 3、不揮発性メモリ 3 4、RTC 3 5、ROM 3 6 以外に、RAM 3 3 に対する書き込みと読み出しを制御する RAM コントローラ 3 0 1、並びに論理回路 3 0 2 を有している。論理回路 3 0 2 は、例えば、暗号化されているコンテンツを解読した後、解読したデータをアダプタ 2 6 から直接出力するような場合の処理のために用いられる。

【0 2 7 2】これらのインタフェース 3 1 乃至 ROM 3 6、RAM コントローラ 3 0 1、並びに論理回路 3 0 2 は、半導体 IC 内に一体的に組み込まれ、外部からは分解できないように構成されている。

【0 2 7 3】水晶振動子 3 1 1 は、アダプタ 2 6 が各種の処理を実行する上において、基準となるクロックを生成するとき用いられる。発振回路 3 1 2 は、RTC 3 5 を動作させるための発振回路である。バッテリー 3 1 3 は、発振回路 3 1 2、不揮発性メモリ 3 4、および RTC 3 5 に対してバックアップ用の電力を供給している。アダプタ 2 6 のその他の回路には、パーソナルコンピュータ 1

の電源供給回路 321 からの電力が供給されている。

【0274】不揮発性メモリ 34 は、書き込み消去可能な ROM で構成することも可能であるが、バッテリー 313 からのバックアップ電源でバックアップされる RAM で構成する場合には、例えば、図 36 に示すように、不揮発性メモリ 34 の上に保護アルミニウム層 351 を形成し、さらに、その保護アルミニウム層 351 と同一平面上となるように、不揮発性メモリ 34 にバッテリー 313 からの電力を供給する電源パターン 352 を形成することができる。このようにすると、例えば、不揮発性メモリ 34 を改竄すべく、保護アルミニウム層 351 を削除しようとする、同一平面上の電源パターン 352 も削除されてしまい、不揮発性メモリ 34 に対する電力の供給が断たれ、内部に記憶されているデータが消去されてしまうことになる。このように構成することで、タンパーレジスト性をより高めることができる。

【0275】さらに、図 37 に示すように、不揮発性メモリ 34 に対するデータの書き込みまたは読み出しのための配線 401-1 乃至 401-3 は、対応する位置で、上下（深さ）方向に重なりあうように形成されている。これにより、より下層の配線 401-3 からデータを読み出すためには、上方の配線 401-1、401-2 を除去しなければならず、複数の配線 401-1、401-2、401-3 から同時にデータを読み取ることができなくなる。

【0276】さらにまた、不揮発性メモリ 34 は、配線 401-1 乃至 401-3 を冗長に形成することができる。例えば、不揮発性メモリ 34 内部に形成される配線 401-1 乃至 401-3 が不揮発性メモリ 34 を構成するトランジスタなどの素子を結合するとき、その経路は、例え、直線的に結合が可能であっても、直線的には形成されず、所定の長さとなるように形成される。このようにすることで、配線 401-1 乃至 401-3 の長さは、本来必要な長さ以上の長さとなり、配線に必要な最短の長さの場合に比較して大きな寄生容量を有することとなる。

【0277】不揮発性メモリ 34 からデータを読み出すために設計されている専用の回路（半導体 IC としてのアダプタ 26 に内蔵されている）は、その寄生容量にマッチングしたインピーダンスを設定することで、不揮発性メモリ 34 が記憶しているデータを正常に読み出すことができる。しかしながら、不揮発性メモリ 34 に記憶されているデータを読み出すべく、プローブを配線 401-1 乃至 401-3 に接続させると、その寄生容量とプローブによる合成の容量が影響して、データを正常に読み出すことが困難になる。

【0278】次に、ポータブルデバイス 6 がパーソナルコンピュータ 1 から所定のデータを受け取る場合の、相互認証の処理を図 38 および図 39 のフローチャートを参照して説明する。ステップ S401 において、パーソ

ナルコンピュータ 1 の CPU 11 は、乱数 Na を生成する。ステップ S402 において、パーソナルコンピュータ 1 の CPU 11 は、インターフェース 17 に、パーソナルコンピュータ 1 の ID、鍵のカテゴリ番号 G、および乱数 Na をポータブルデバイス 6 へ送信させる。

【0279】ステップ S421 において、ポータブルデバイス 6 の CPU 53 は、乱数 Nb を生成する。ステップ S422 において、ポータブルデバイス 6 は、USB コントローラ 57 を介して、パーソナルコンピュータ 1 から送信されたパーソナルコンピュータ 1 の ID、鍵のカテゴリ番号 G、および乱数 Na を受信する。ステップ S423 において、ポータブルデバイス 6 の CPU 53 は、鍵のカテゴリ番号 G から、マスター鍵  $K_{m,j}$  の鍵番号 j を求める。

【0280】ステップ S424 において、ポータブルデバイス 6 の CPU 53 は、j 番目のマスター鍵  $K_{m,j}$  を求める。ステップ S425 において、ポータブルデバイス 6 の CPU 53 は、パーソナルコンピュータ 1 の ID に、マスター鍵  $K_{m,j}$  を基にした SHA などのハッシュ関数を適用し、鍵  $K_{m,j}$  を求める。

【0281】ステップ S426 において、ポータブルデバイス 6 の CPU 53 は、乱数 Na、乱数 Nb、およびパーソナルコンピュータ 1 の ID に、鍵  $K_{m,j}$  を基にした SHA などのハッシュ関数を適用し、乱数 R1 を求める。ステップ S427 において、ポータブルデバイス 6 の CPU 53 は、乱数 Sb を生成する。

【0282】ステップ S428 において、ポータブルデバイス 6 の CPU 53 は、USB コントローラ 57 に、乱数 Na、乱数 Nb、鍵番号 j、および乱数 Sb をパーソナルコンピュータ 1 へ送信させる。

【0283】ステップ S403 において、パーソナルコンピュータ 1 は、インターフェース 17 を介して、乱数 Na、乱数 Nb、鍵番号 j、および乱数 Sb を受信する。ステップ S404 において、パーソナルコンピュータ 1 の CPU 11 は、鍵番号 j を基に、個別鍵  $K_{i,j}$  に含まれる鍵  $K_{m,j}$  を求める。ステップ S405 において、パーソナルコンピュータ 1 の CPU 11 は、乱数 Na、乱数 Nb、およびパーソナルコンピュータ 1 の ID に、鍵  $K_{m,j}$  を基にした SHA などのハッシュ関数を適用し、乱数 R2 を求める。

【0284】ステップ S406 において、パーソナルコンピュータ 1 の CPU 11 は、受信した乱数 R1 と、ステップ S405 で生成した乱数 R2 とが等しいか否かを判定し、乱数 R1 と乱数 R2 とが等しくない判定された場合、正当なポータブルデバイスではないので、ポータブルデバイス 6 を認証せず、処理は終了する。ステップ S406 において、乱数 R1 と乱数 R2 とが等しいと判定された場合、ポータブルデバイス 6 は正当なポータブルデバイスなので、ステップ S407 に進み、パーソナルコンピュータ 1 の CPU 11 は、乱数 Sa を生成する。

【0285】ステップS408において、パーソナルコンピュータ1のCPU11は、乱数Nbおよび乱数Naに、鍵K<sub>u</sub>を基にしたSHAなどのハッシュ関数を適用し、乱数R3を求める。ステップS409において、パーソナルコンピュータ1のCPU11は、インターフェース17に、乱数R3および乱数Sbをポータブルデバイス6へ送信させる。ステップS410において、パーソナルコンピュータ1のCPU11は、乱数Saおよび乱数Sbに、鍵K<sub>u</sub>を基にしたSHAなどのハッシュ関数を適用し、一時鍵K<sub>s</sub>を求める。

【0286】ステップS429において、ポータブルデバイス6のCPU53は、USBコントローラ57を介して、乱数R3および乱数Sbを受信する。ステップS430において、ポータブルデバイス6のCPU53は、乱数Nbおよび乱数Naに、鍵K<sub>u</sub>を基にしたSHAなどのハッシュ関数を適用し、乱数R4を求める。ステップS431において、ポータブルデバイス6のCPU53は、受信した乱数R3と、ステップS430で生成した乱数R4とが等しいか否かを判定し、乱数R3と乱数R4とが等しくないかと判定された場合、正当なパーソナルコンピュータではないので、パーソナルコンピュータ1を認証せず、処理は終了する。ステップS431において、乱数R3と乱数R4とが等しいと判定された場合、パーソナルコンピュータ1は正当なパーソナルコンピュータなので、ステップS432に進み、ポータブルデバイス6のCPU53は、乱数Saおよび乱数Sbに、鍵K<sub>u</sub>を基にしたSHAなどのハッシュ関数を適用し、一時鍵K<sub>s</sub>を求める。

【0287】以上のように、パーソナルコンピュータ1およびポータブルデバイス6は、相互認証し、共通の一時鍵K<sub>s</sub>を得る。なお、ステップS425、ステップS426、ステップS405、ステップS408、ステップS410、ステップS430、およびステップS432において、SHAなどのハッシュ関数を適用するとして説明したが、DESなどを適用しても良い。

【0288】次に、パーソナルコンピュータ1がポータブルデバイス6に所定のデータを送信する場合の、相互認証の処理を図40および図41のフローチャートを参照して説明する。ステップS451において、パーソナルコンピュータ1のCPU11は、乱数Naを生成する。ステップS452において、パーソナルコンピュータ1は、インターフェース17を介して、パーソナルコンピュータ1のID、パーソナルコンピュータ1の鍵のカテゴリ番号Gp、ポータブルデバイス6の鍵のカテゴリ番号Gs、および乱数Naをポータブルデバイス6に送信する。

【0289】ステップS481において、ポータブルデバイス6のCPU53は、乱数Nbを生成する。ステップS482において、ポータブルデバイス6は、USBコントローラ57を介して、パーソナルコンピュータ1から

送信されたパーソナルコンピュータ1のID、パーソナルコンピュータ1の鍵のカテゴリ番号Gp、ポータブルデバイス6の鍵のカテゴリ番号Gs、および乱数Naを受信する。ステップS483において、ポータブルデバイス6のCPU53は、ポータブルデバイス6の鍵のカテゴリ番号Gsから、マスター鍵K<sub>u</sub>の鍵番号jを求める。

【0290】ステップS484において、ポータブルデバイス6のCPU53は、j番目のマスター鍵K<sub>u(j)</sub>を求める。ステップS485において、ポータブルデバイス6のCPU53は、パーソナルコンピュータ1のIDに、マスター鍵K<sub>u(j)</sub>を基にしたSHAなどのハッシュ関数を適用ハッシュ関数を適用し、鍵K<sub>s</sub>を求める。ステップS486において、ポータブルデバイス6のCPU53は、パーソナルコンピュータ1の鍵のカテゴリ番号Gpを基に、マスター鍵K<sub>i</sub>の鍵番号kを求める。ステップS487において、ポータブルデバイス6のCPU53は、鍵K<sub>s</sub>に、マスター鍵K<sub>i(k)</sub>を基にしたSHAなどのハッシュ関数を適用ハッシュ関数を適用し、鍵K'を求める。

【0291】ステップS488において、ポータブルデバイス6のCPU53は、乱数Naおよび乱数Nbに、鍵K'を基にしたSHAなどのハッシュ関数を適用ハッシュ関数を適用し、乱数R1を求める。ステップS489において、ポータブルデバイス6のCPU53は、乱数Sbを生成する。

【0292】ステップS490において、ポータブルデバイス6のCPU53は、USBコントローラ57に、ポータブルデバイス6のID、乱数Nb、乱数R1、鍵番号j、および乱数Sbをパーソナルコンピュータ1へ送信させる。

【0293】ステップS453において、パーソナルコンピュータ1は、インターフェース17を介して、ポータブルデバイス6のID、乱数Nb、乱数R1、鍵番号j、および乱数Sbを受信する。ステップS454において、パーソナルコンピュータ1のCPU11は、ポータブルデバイス6のIDに、パーソナルコンピュータ1のマスター鍵K<sub>u</sub>を基にしたSHAなどのハッシュ関数を適用ハッシュ関数を適用し、マスター鍵K<sub>s</sub>を求める。ステップS455において、パーソナルコンピュータ1のCPU11は、j番目の個別鍵K<sub>i</sub>を求める。ステップS456において、パーソナルコンピュータ1のCPU11は、乱数Naおよび乱数Nbに、鍵K<sub>s</sub>を基にしたSHAなどのハッシュ関数を適用ハッシュ関数を適用し、鍵K'を求める。ステップS457において、パーソナルコンピュータ1のCPU11は、乱数Naおよび乱数Nbに、鍵K'を基にしたSHAなどのハッシュ関数を適用ハッシュ関数を適用し、乱数R2を求める。

【0294】ステップS458において、パーソナルコンピュータ1のCPU11は、受信した乱数R1と、ステップS457で生成した乱数R2とが等しいか否かを判

定し、乱数 R 1 と乱数 R 2 とが等しくないとは判定された場合、正当なポータブルデバイスではないので、ポータブルデバイス 6 を認証せず、処理は終了する。ステップ S 4 5 8 において、乱数 R 1 と乱数 R 2 とが等しいとは判定された場合、ポータブルデバイス 6 は正当なポータブルデバイスなので、ステップ S 4 5 9 に進み、パーソナルコンピュータ 1 の CPU 1 1 は、乱数 S a を生成する。

【0295】ステップ S 4 6 0 において、パーソナルコンピュータ 1 の CPU 1 1 は、乱数 N b および乱数 N a に、鍵 K<sub>1</sub> を基にした SHA などのハッシュ関数を適用し、乱数 R 3 を求める。ステップ S 4 6 1 において、パーソナルコンピュータ 1 の CPU 1 1 は、インターフェース 1 7 を介して、ポータブルデバイス 6 に、乱数 R 3 および乱数 S b を送信する。ステップ S 4 6 2 において、パーソナルコンピュータ 1 の CPU 1 1 は、乱数 S a および乱数 S b に、鍵 K' を基にした SHA などのハッシュ関数を適用し、一時鍵 K<sub>s</sub> を求める。

【0296】ステップ S 4 9 1 において、ポータブルデバイス 6 の CPU 5 3 は、USB コントローラ 5 7 を介して、乱数 R 3 および乱数 S b を受信する。ステップ S 4 9 2 において、ポータブルデバイス 6 の CPU 5 3 は、乱数 N b および乱数 N a に、鍵 K<sub>1</sub> を基にした SHA などのハッシュ関数を適用し、乱数 R 4 を求める。ステップ S 4 9 3 において、ポータブルデバイス 6 の CPU 5 3 は、受信した乱数 R 3 と、ステップ S 4 9 2 で生成した乱数 R 4 とが等しいかを判定し、乱数 R 3 と乱数 R 4 とが等しくないとは判定された場合、正当なパーソナルコンピュータではないので、パーソナルコンピュータ 1 を認証せず、処理は終了する。ステップ S 4 9 3 において、乱数 R 3 と乱数 R 4 とが等しいとは判定された場合、パーソナルコンピュータ 1 は、正当なパーソナルコンピュータなので、ステップ S 4 9 4 に進み、ポータブルデバイス 6 の CPU 5 3 は、乱数 S a および乱数 S b に、鍵 K<sub>1</sub> を基にした SHA などのハッシュ関数を適用し、一時鍵 K<sub>s</sub> を求める。

【0297】このように、パーソナルコンピュータ 1 およびポータブルデバイス 6 は、相互認証し、共通の一時鍵 K<sub>s</sub> を得る。図 4 0 および図 4 1 のフローチャートに示した手続きは、図 3 8 および図 3 9 のフローチャートに示す手続きよりも、いわゆる「なりすまし」に対する防御（検出）が強力である。なお、ステップ S 4 8 5、ステップ S 4 8 7、ステップ S 4 8 8、ステップ S 4 5 4、ステップ S 4 5 6、ステップ S 4 5 7、ステップ S 4 6 0、ステップ S 4 6 2、ステップ S 4 9 2、およびステップ S 4 9 4 において、SHA などのハッシュ関数を適用するとして説明したが、DES などを適用しても良い。

【0298】以上のように、パーソナルコンピュータ 1 およびポータブルデバイス 6 は、相互認証の後に行われ

る処理に対応し、検出力が異なる相互認証の手続きを使い分けることにより、効率的かつ強力に、なりすましによる攻撃に対応することができる。

【0299】次に、ソースプログラムを暗号化する処理を、図 4 2 のフローチャートを参照して説明する。ステップ S 5 0 1 において、パーソナルコンピュータ 1 は、インターネット接続インターフェース 1 1 を介して、図示せぬ認証局に署名を付したソースプログラムを送信する。ステップ S 5 0 2 において、認証局は、署名を基に、受信したソースプログラムに改竄が発見されたか否かを判定し、受信したソースプログラムに改竄が発見された場合、処理は継続できないので、処理は終了する。

【0300】ステップ S 5 0 2 において、受信したソースプログラムに改竄が発見されなかった場合、ステップ S 5 0 3 に進み、認証局は、受信したソースプログラムを認証局の秘密鍵で暗号化する。ステップ S 5 0 4 において、認証局は、暗号化したソースプログラムをパーソナルコンピュータ 1 に送信する。ステップ S 5 0 5 において、パーソナルコンピュータ 1 は、受信したソースプログラムを、HDD 2 1 に記録し、処理は終了する。

【0301】以上のように、ソースプログラムは、暗号化される。なお、認証局に代わり、EMD サーバ 4 または所定の安全なサーバが、ソースプログラムを暗号化するようにしてもよい。

【0302】次に、暗号化されたソースプログラムをアダプタ 2 6 が実行する処理を、図 4 3 のフローチャートを参照して説明する。ステップ S 5 2 1 において、アダプタ 2 6 の CPU 3 2 は、パーソナルコンピュータ 1 から受信した、暗号化されたソースプログラムを、不揮発性メモリ 3 4 に予め記憶されている認証局の公開鍵で復号する。ステップ S 5 2 2 において、アダプタ 2 6 の CPU 3 2 は、インタープリタを起動し、復号されたソースプログラムを実行する。

【0303】ステップ S 5 2 3 において、アダプタ 2 6 の CPU 3 2 は、ソースプログラムを実行して得られた結果を、パーソナルコンピュータ 1 に送信するか否かを判定し、結果をパーソナルコンピュータ 1 に送信しないと判定された場合、処理は終了する。ステップ S 5 2 3 において、結果をパーソナルコンピュータ 1 に送信すると判定された場合、ステップ S 5 2 4 に進み、アダプタ 2 6 の CPU 3 2 は、ソースプログラムを実行して得られた結果を所定の鍵で暗号化する。ステップ S 5 2 5 において、アダプタ 2 6 の CPU 3 2 は、インターフェース 3 1 を介して、暗号化された結果をパーソナルコンピュータ 1 に送信し、処理は終了する。

【0304】以上のように、アダプタ 2 6 は、暗号化されたソースプログラムを実行し、所定の鍵で得られた結果を暗号化し、パーソナルコンピュータ 1 に送信する。

【0305】なお、オブジェクトプログラムを暗号化

し、暗号化されたオブジェクトプログラムをアダプタ 26 が実行するようにしてもよい。図 44 は、オブジェクトプログラムを暗号化する処理を説明するフローチャートである。ステップ S541 において、パーソナルコンピュータ 1 は、ソースプログラムをコンパイルし、所定のオブジェクトプログラムを生成する。ステップ S542 乃至ステップ S546 の処理は、図 42 のステップ S501 乃至ステップ S505 とそれぞれ同様の処理なので、その説明は省略する。

【0306】図 45 は、暗号化されたオブジェクトプログラムをアダプタ 26 が実行する処理を説明するフローチャートである。ステップ S561 において、アダプタ 26 の CPU32 は、パーソナルコンピュータ 1 から受信した、暗号化されたオブジェクトプログラムを、不揮発性メモリ 34 に予め記憶されている認証局の公開鍵で復号する。ステップ S562 において、アダプタ 26 の CPU32 は、復号されたオブジェクトプログラムを RAM33 に展開し、実行する。ステップ S563 乃至ステップ S565 は、図 43 のステップ S523 乃至ステップ S525 とそれぞれ同様の処理なので、その説明は省略する。

【0307】次に、オブジェクトプログラムを暗号化する他の処理を、図 46 のフローチャートを参照して説明する。ステップ S581 において、パーソナルコンピュータ 1 の CPU11 は、ソースプログラムをコンパイルし、オブジェクトプログラムを生成する。ステップ S582 において、パーソナルコンピュータ 1 の CPU11 は、インターフェース 17 を介して、アダプタ 26 にアプリケーション鍵 K<sub>ap</sub> および個別鍵 K<sub>idv</sub> の発行を要求する。

【0308】ステップ S583 において、パーソナルコンピュータ 1 は、インターフェース 17 を介して、アダプタ 26 からアプリケーション鍵 K<sub>ap</sub> および個別鍵 K<sub>idv</sub> (アダプタ 26 の不揮発性メモリ 34 に記憶されている、アダプタ 26 固有の鍵 K<sub>s</sub> を基に、生成される) を受信する。ステップ S584 において、パーソナルコンピュータ 1 の CPU11 は、オブジェクトプログラムをアプリケーション鍵 K<sub>ap</sub> で暗号化する。ステップ S585 において、パーソナルコンピュータ 1 の CPU11 は、コンテキストに含まれるマスター鍵 K<sub>m</sub> など個別鍵 K<sub>idv</sub> で暗号化する。ステップ S586 において、パーソナルコンピュータ 1 の CPU11 は、アプリケーション鍵 K<sub>ap</sub> で暗号化されたオブジェクトプログラム、および個別鍵 K<sub>idv</sub> で暗号化されたコンテキストに含まれるマスター鍵 K<sub>m</sub> など HDD21 に記録させ、処理は終了する。

【0309】このように、パーソナルコンピュータ 1 は、アダプタ 26 から供給されたアプリケーション鍵 K<sub>ap</sub> および個別鍵 K<sub>idv</sub> で、オブジェクトプログラムおよびコンテキストを暗号化することができる。

【0310】図 46 のフローチャートに示される手順で

暗号化されたオブジェクトプログラムをアダプタ 26 が実行する処理を、図 47 のフローチャートを参照して説明する。ステップ S601 において、パーソナルコンピュータ 1 の CPU11 は、インターフェース 17 を介して、アダプタ 26 に、アプリケーション鍵 K<sub>ap</sub> で暗号化されたオブジェクトプログラム、および個別鍵 K<sub>idv</sub> で暗号化されたコンテキストに含まれるマスター鍵 K<sub>m</sub> などを送信する。

【0311】ステップ S602 において、アダプタ 26 の CPU32 は、不揮発性メモリ 34 に予め記憶されている鍵 K<sub>s</sub> およびアプリケーション鍵 K<sub>ap</sub> に、ハッシュ関数を適用し、個別鍵 K<sub>idv</sub> を生成する。ステップ S603 において、アダプタ 26 の CPU32 は、受信したオブジェクトプログラムをアプリケーション鍵 K<sub>ap</sub> で復号する。ステップ S604 において、アダプタ 26 の CPU32 は、コンテキストに含まれるマスター鍵 K<sub>m</sub> など個別鍵 K<sub>idv</sub> で復号する。

【0312】ステップ S605 において、アダプタ 26 の CPU32 は、復号されたマスター鍵 K<sub>m</sub> などを含むコンテキストを利用して、オブジェクトプログラムを実行する。ステップ S606 乃至ステップ S608 の処理は、図 43 のステップ S523 乃至ステップ S525 とそれぞれ同様の処理なので、その説明は省略する。

【0313】以上のように、図 47 のフローチャートで示される処理において、図 46 のフローチャートで個別鍵 K<sub>idv</sub> を送信したアダプタ 26 は、暗号化されたオブジェクトプログラムを実行することができる。従って、図 46 のフローチャートで個別鍵 K<sub>idv</sub> を送信したアダプタ 26 以外のアダプタは、オブジェクトプログラムを復号できるが、コンテキストを復号できず、暗号化されたオブジェクトプログラムは実行できない。

【0314】次に、アダプタ 26 がオブジェクトプログラムを実行する場合、処理の一部をパーソナルコンピュータ 1 の CPU11 に実行させるときの処理を図 48 のフローチャートを参照して説明する。ステップ S651 において、アダプタ 26 の CPU32 は、オブジェクトプログラムの所定の命令列を、所定の規則に従って、変換する。

【0315】この変換は、例えば、DES の暗号化または復号のプログラムの場合、Feistel 構造などの基本構造を繰り返す処理のとき、いわゆる F 関数で利用される 48 ビットの拡大鍵と適切な乱数とに排他的論理和を所定の回数、適用するなどの変換を実行し、拡大鍵を解読しにくくする。また、例えば、DES CBC (Cipher Block Chaining) Mode で、多量のデータを復号するプログラムの場合、繰り返す構造の処理を順 (シーケンシャル) に実行せず、多量のデータに対し、複数の繰り返し構造の処理を同時に実行し、拡大鍵を解読しにくくする。

【0316】また、例えば、ソースプログラムのインス

トランクションに対応するコード（例えば、加算を表すコードが” 1” に対応し、乗算を表すコードが” 2” に対応する）を毎回変更する。

【 0 3 1 7 】ステップ S 6 5 2 において、アダプタ 2 6 の CPU 3 2 は、変換された命令列を、インターフェース 3 1 を介して、パーソナルコンピュータ 1 に送信する。

【 0 3 1 8 】ステップ S 6 5 3 において、パーソナルコンピュータ 1 の CPU 1 1 は、デジャッフルされた命令列を実行する。ステップ S 6 5 4 において、パーソナルコンピュータ 1 の CPU 1 1 は、命令列を実行して得られた 10 処理結果をアダプタ 2 6 に送信する。

【 0 3 1 9 】ステップ S 6 5 5 において、アダプタ 2 6 の CPU 3 2 は、パーソナルコンピュータ 1 から受信した処理結果、およびアダプタ 2 6 の CPU 3 2 が算出し保持している計算結果を基に、処理を継続する。ステップ S 6 5 6 において、アダプタ 2 6 の CPU 3 2 は、パーソナルコンピュータ 1 に処理を実行させるか否かを判定し、パーソナルコンピュータ 1 に処理を実行させないと判定された場合、処理は終了する。ステップ S 6 5 6 において、パーソナルコンピュータ 1 に処理を実行させると判定された場合、手続きは、ステップ S 6 5 1 に戻り、パーソナルコンピュータ 1 に処理を実行させる処理を繰り返す。 20

【 0 3 2 0 】以上のように、アダプタ 2 6 は、オブジェクトプログラムの処理の一部をパーソナルコンピュータ 1 に実行させることにより、高速にかつ安全に、オブジェクトプログラムの処理を実行することができる。

【 0 3 2 1 】アダプタ 2 6 は、オブジェクトプログラムに含まれる命令列を変換してパーソナルコンピュータ 1 に送信することにより、オブジェクトプログラムの解読が困難になる。アダプタ 2 6 が、オブジェクトプログラムに含まれる命令列を暗号化して、パーソナルコンピュータ 1 に送信すれば、オブジェクトプログラムの解読は更に困難になる。 30

【 0 3 2 2 】なお、図 4 6 で説明したパーソナルコンピュータ 1 がアダプタ 2 6 に供給するオブジェクトプログラムを暗号化する処理において、ソースプログラムに対してステップ S 6 5 1 に示した変換を実行すれば、オブジェクトプログラムの解読は更に困難になる。

【 0 3 2 3 】最後に、パーソナルコンピュータ 1 が EMD サーバ 4 から、事前に無料でダウンロードしたコンテンツを暗号化している暗号鍵をダウンロードするとともに、決済をする処理を、図 4 9 のフローチャートを参照して説明する。ステップ S 6 7 1 において、パーソナルコンピュータ 1 は、インターネット 4 を介して、EMD サーバ 4 と相互認証する。ステップ S 6 7 2 において、パーソナルコンピュータ 1 の CPU 1 1 は、インターネット 4 を介して、EMD サーバ 4 に、コンテンツの再生条件を示すデータを送信する。ステップ S 6 7 3 において、EMD サーバ 4 は、受信した再生条 40

件を示すデータを基に、支払い金額のデータをパーソナルコンピュータ 1 に送信する。

【 0 3 2 4 】ステップ S 6 7 4 において、パーソナルコンピュータ 1 の CPU 1 1 は、EMD サーバ 4 から受信した支払い金額のデータをディスプレイ 3 に表示させる。ステップ S 6 7 5 において、EMD サーバ 4 は、パーソナルコンピュータ 1 に、ユーザのクレジットカードの番号等の送信を要求する。ステップ S 6 7 6 において、ユーザは、入力部 2 を操作し、パーソナルコンピュータ 1 にクレジットカードの番号等のデータを入力し、パーソナルコンピュータ 1 は、クレジットカードの番号等のデータを EMD サーバ 4 に送信する。

【 0 3 2 5 】ステップ S 6 7 7 において、EMD サーバ 4 は、パーソナルコンピュータ 1 から受信したクレジットカードの番号等のデータを基に、決済の処理を実行する。ステップ S 6 7 8 において、EMD サーバ 4 は、インターネット 4 を介して、パーソナルコンピュータ 1 に所定の暗号鍵を送信する。ステップ S 6 7 9 において、パーソナルコンピュータ 1 は、インターネット 4 を介して、EMD サーバ 4 から送信された所定の暗号鍵を受信し、処理は終了する。

【 0 3 2 6 】以上のように、パーソナルコンピュータ 1 が EMD サーバ 4 から暗号鍵をダウンロードするとともに、EMD サーバ 4 は、決済の処理をすれば、パーソナルコンピュータ 1 が EMD サーバ 4 からコンテンツをダウンロードするとき、認証、暗号化、または決済などの処理が必要なくなるので、比較的大きなデータであるコンテンツを迅速にダウンロードすることができる。

【 0 3 2 7 】以上においては、記録媒体として、ポータブルデバイス 6 を用いる場合を例として説明したが、本発明は、その他の記録媒体にデータを移転またはコピーする場合にも応用することが可能である。クレジットカードの番号等のデータを基に、決済の処理を実行して説明したが、s m a s h（商標）などの手続きにより、決済をするようにしてもよい。

【 0 3 2 8 】また、図 4 9 のフローチャートに示す処理の前に、パーソナルコンピュータ 1 と EMD サーバ 4 とが、例えば、IS09798-3 で規定されている http (Hypertext Transport Protocol) 上のプロトコルを使用して、相互認証するようにしてもよい。

【 0 3 2 9 】なお、ポータブルデバイス 6 は、予め個別鍵を記憶しているとして説明したが、ユーザがポータブルデバイス 6 を購入後、EMD サーバ 4 などからダウンロードするようにしてもよい。

【 0 3 3 0 】以上においては、記録媒体として、ポータブルデバイス 6 を用いる場合を例として説明したが、本発明は、その他の記録媒体にデータを移転またはコピーする場合にも応用することが可能である。

【 0 3 3 1 】また、コンテンツは、曲のデータまたは音声データなどの楽音データ以外に、画像データ、その他 50

のデータとすることもできる。

【0332】以上のように、本発明によれば、次のような効果を奏することができる。

【0333】(1) HDD21に暗号化してデータを記録するとともに、暗号鍵も保存用鍵で暗号化した上でHDD21に記録するようにしたので、HDD21に記録されているコンテンツをコピーしても、これを復号することができないので、複製が大量に配布されることを防止することができる。

【0334】(2) 所定の曲を1回コピーしたとき、一定時間(上記例の場合、48時間)の間、その曲をコピーすることができないようするために、その曲と録音日時を曲データベース上に登録するようにしたので、そのコピー回数を制限することができ、複製を大量に配布することを防止することができる。

【0335】さらにデータベースを更新する度に、データのハッシュ値を計算し保存するようにしたので、データベースの改竄を防止することが容易となる。

【0336】(3) 外部の装置にコンテンツを渡したら、HDD21上のコンテンツを消去するようにしたので、HDD21内に元のデジタルデータであるコンテンツが残らず、その複製を大量に配布することが防止される。

【0337】(4) HDD21内に曲データベースを設け、全体のハッシュ値を毎回チェックするようにしたので、HDD21の内容をムーブの直前にバックアップし、ムーブ直後にバックアップしたデータをHDD21にリストアするようにしたとしても、送り元のデータを確実に消去することが可能となる。

【0338】(5) パーソナルコンピュータ1が外部の機器にデータを渡すとき、その前に相互認証処理を行うようにしたので、不正な機器にデータを渡してしまうようなことが防止される。

【0339】(6) 外部機器から、パーソナルコンピュータ1に対してデータを渡す前に、パーソナルコンピュータ1のソフトウェアが正当なものであるか否かを相互認証により確認するようにしたので、不正なソフトウェアに対してコンテンツを渡してしまうようなことが防止される。

【0340】(7) 曲の同一性の判定にISRCを用い、ISRCが取得できないときは、TOCを用いるようにしたので、ISRCが取得できなくとも、曲の同一性を判定することが可能になる。

【0341】(8) パーソナルコンピュータ1におけるソフトウェア機能のうち、所定の部分をパーソナルコンピュータ1に外付けされるアダプタ26に負担させるようにしたので、パーソナルコンピュータ1のソフトウェアを解析しただけでは、全体としてどのような処理となっているのかが判らないので、ソフトウェアを改竄して、意図する機能を持たせるようなことが困難とな

る。

【0342】(9) プログラムをプログラムに対応する鍵で暗号化し、プログラムの実行に必要なデータを、アダプタ26が生成する固有の鍵で暗号化するようにしたので、プログラムのみをCD-ROMなどの媒体で配布可能にしつつ、プログラムを他のアダプタ26で実行することが防止される。

【0343】(10) 音楽データなどのコンテンツを暗号化する鍵をダウンロードするとき、決済されるようにしたので、比較的大きなデータである音楽データなどのコンテンツを迅速にダウンロードすることができるようになる。

【0344】なお、アダプタ26が実行する処理は、セキュアなプログラムでCPU11が実行するようにしてもよい。この場合において、例えば、同一な値を有する保存用鍵は、保存用鍵が必要になった時点で、コンテンツ管理プログラム111により生成される。同様に、ハッシュ値は、コンテンツ管理プログラム111により隠蔽されて保存される。

【0345】また、アダプタ26が実行する処理が、セキュアなプログラムでCPU11により実行されるとき、パーソナルコンピュータ1は、アダプタ26のRTC35が供給する現在時刻に代えて、ネットワーク2に接続されている特定のサーバ(例えば、EMD登録サーバ3)から現在時刻のデータをダウンロードして、その現在時刻を基に、判定の処理を実行する。また、この場合において、パーソナルコンピュータ1は、所定の時間間隔で現在時刻を記憶して、記憶している時刻より以前の時刻が設定されたとき、エラーの表示を行い、時刻の設定を受け付けないようにしてもよい。

【0346】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

【0347】コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図2に示すように、磁気ディスク41(フロッピディスクを含む)、光ディスク42(CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む)、光磁気ディスク43(MD(Mini-Disc)を含む)、若しくは半導体メモリ44などよりなるパッケージメディア、または、プログラムが一時的若しくは永続的に格納されるROM12や、HDD21などにより構成される。プログラム格納媒体へのプログラムの格納は、必要に応じて通信部25な

どのインタフェースを介して、ローカルエリアネットワークまたはインターネットなどのネットワーク 2、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

【0348】なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0349】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0350】

【発明の効果】請求項 1 に記載の情報処理装置、請求項 4 に記載の情報処理方法、および請求項 5 に記載のプログラム格納媒体によれば、半導体 IC に実行させるプログラムに含まれる命令列が並び替えられ、プログラムが暗号化され、命令列が並び替えられ、暗号化されたプログラムが記録され、記録されているプログラムが、半導体 IC に送信されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

【図面の簡単な説明】

【図 1】本発明に係るコンテンツデータ管理システムの一実施の形態を示す図である。

【図 2】パーソナルコンピュータ 1 の構成を説明する図である。

【図 3】ポータブルデバイス 6 の構成を説明する図である。

【図 4】パーソナルコンピュータ 1 の機能の構成を説明するブロック図である。

【図 5】表示操作指示ウィンドウの例を示す図である。

【図 6】録音プログラム 113 がディスプレイ 20 に表示させるウィンドウの例を説明する図である。

【図 7】コンパクトディスクから HDD 21 にコンテンツをコピーする場合の処理を説明するフローチャートである。

【図 8】図 7 のステップ S12 の期限データベースチェック処理を説明するフローチャートである。

【図 9】期限データベースの例を示す図である。

【図 10】ウォータマークを説明する図である。

【図 11】曲データベースの例を示す図である。

【図 12】HDD 21 からポータブルデバイス 6 へコンテンツを移動する動作を説明するフローチャートである。

【図 13】HDD 21 からポータブルデバイス 6 へコンテンツを移動する動作を説明するフローチャートである。

【図 14】HDD 21 からポータブルデバイス 6 へコンテンツを移動する動作を説明するフローチャートである。

【図 15】図 12 のステップ S55 の選択されたコンテンツの再生条件などのチェック処理を説明するフロー

チャートである。

【図 16】ポータブルデバイス 6 が管理している再生条件を説明する図である。

【図 17】図 12 のステップ S58 のフォーマット変換処理の詳細を説明するフローチャートである。

【図 18】HDD 21 からポータブルデバイス 6 へコンテンツをコピーする場合の動作を説明するフローチャートである。

【図 19】HDD 21 からポータブルデバイス 6 へコンテンツをコピーする場合の動作を説明するフローチャートである。

【図 20】HDD 21 からポータブルデバイス 6 へコンテンツをコピーする場合の動作を説明するフローチャートである。

【図 21】ポータブルデバイス 6 から HDD 21 へコンテンツを移動する場合の動作を説明するフローチャートである。

【図 22】ポータブルデバイス 6 から HDD 21 へコンテンツをコピーする場合の動作を説明するフローチャートである。

【図 23】EMD サーバ 4 から HDD 21 へコンテンツをコピーする場合の処理を説明するフローチャートである。

【図 24】図 23 のステップ S204 の課金に関する処理の詳細を説明するフローチャートである。

【図 25】課金ログを説明する図である。

【図 26】図 2 のパーソナルコンピュータ 1 の IEC60958 端子 24a から HDD 21 へコンテンツをコピーする場合の処理を説明するフローチャートである。

【図 27】図 2 のパーソナルコンピュータ 1 の IEC60958 端子 24a から HDD 21 へコンテンツをコピーする場合の処理を説明するフローチャートである。

【図 28】HDD 21 から IEC60958 端子 24a にコンテンツを出力する場合の動作を説明するフローチャートである。

【図 29】HDD 21 から IEC60958 端子 24a にコンテンツを出力する場合の動作を説明するフローチャートである。

【図 30】図 28 のステップ S275 の再生条件などのチェック処理を説明するフローチャートである。

【図 31】HDD 21 からポータブルデバイス 6 経由でコンテンツを出力する場合の動作を説明するフローチャートである。

【図 32】HDD 21 からポータブルデバイス 6 経由でコンテンツを出力する場合の動作を説明するフローチャートである。

【図 33】不揮発性メモリ 34 の機能を説明する図である。

【図 34】アダプタ 26 の動作を説明するフローチャートである。

【図 35】アダプタ 26 の内部の構成を示す図である。

【図 36】不揮発性メモリ 34 の内部の構成例を示す図である。

【図 37】不揮発性メモリ 34 の内部の構成例を示す図である。

【図 38】ポータブルデバイス 6 とパーソナルコンピュータ 1 との相互認証の処理を説明するフローチャートである。

【図 39】ポータブルデバイス 6 とパーソナルコンピュータ 1 との相互認証の処理を説明するフローチャートである。

【図 40】ポータブルデバイス 6 とパーソナルコンピュータ 1 との相互認証の処理を説明するフローチャートである。

【図 41】ポータブルデバイス 6 とパーソナルコンピュータ 1 との相互認証の処理を説明するフローチャートである。

【図 42】ソースプログラムを暗号化する処理を説明するフローチャートである。

【図 43】暗号化されたソースプログラムをアダプタ 26 が実行する処理を説明するフローチャートである。

【図 44】オブジェクトプログラムを暗号化する処理を説明するフローチャートである。

【図 45】暗号化されたオブジェクトプログラムをアダプタ 26 が実行する処理を説明するフローチャートである。

【図 46】オブジェクトプログラムを暗号化する他の処理を説明するフローチャートである。

【図 47】暗号化されたオブジェクトプログラムをアダプタ 26 が実行する他の処理を説明するフローチャートである。

【図 48】アダプタ 26 がオブジェクトプログラムを実行する場合、処理の一部をパーソナルコンピュータ 1 の

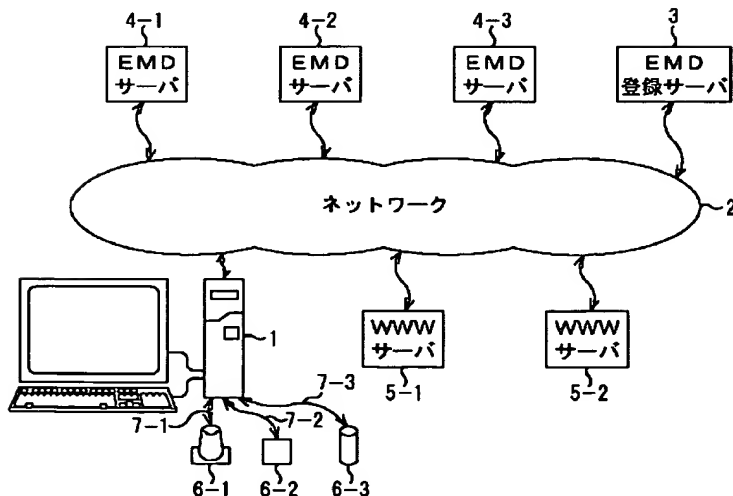
CPU 11 に実行させるときの処理を説明するフローチャートである。

【図 49】パーソナルコンピュータ 1 が EMD サーバ 4 から暗号鍵をダウンロードするとともに、決済をする処理を説明するフローチャートである。

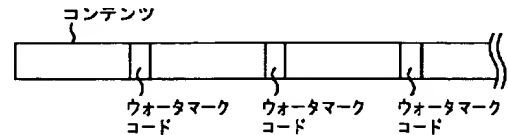
#### 【符号の説明】

- 1 パーソナルコンピュータ, 2 ネットワーク,  
3 EMD登録サーバ, 6-1乃至6-3 ポータブルデバイス, 11 CPU, 12 ROM, 13 RAM, 24 HDD, 24音声入出力インターフェース, 24a IEC60958端子, 26 アダプタ, 32 CPU, 33 RAM, 34 不揮発性メモリ, 35 RTC, 36 ROM, 41 磁気ディスク, 42 光ディスク, 43 光磁気ディスク, 44 半導体メモリ, 53 CPU, 54 RAM, 55 ROM, 59 DSP, 61 フラッシュメモリ, 111 コンテンツ管理プログラム, 112 表示操作指示プログラム, 113 録音プログラム, 114 コンテンツデータベース, 131 EMD選択プログラム, 132 チェックイン/チェックアウト管理プログラム, 133 コピー管理プログラム, 134 移動管理プログラム, 135 暗号方式変換プログラム, 136 圧縮方式変換プログラム, 137 暗号化プログラム, 138 圧縮/伸張プログラム, 139 利用条件変換プログラム, 140 利用条件管理プログラム, 141 認証プログラム, 142 復号プログラム, 143 PD用ドライバ, 144 購入用プログラム, 145 購入用プログラム, 181 フィルタリングデータファイル, 182 表示データファイル, 183 画像ファイル, 184 履歴データファイル, 351 保護アルミニウム層, 352 電源パターン, 401-1乃至401-3配線

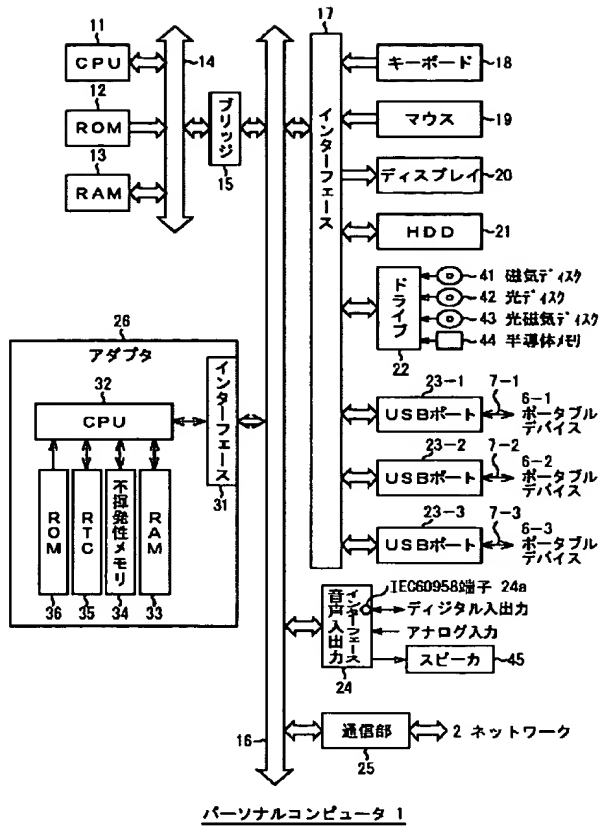
【図 1】



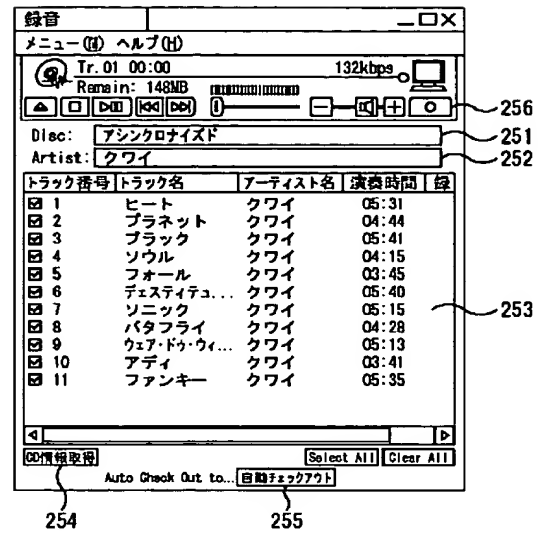
【図 10】



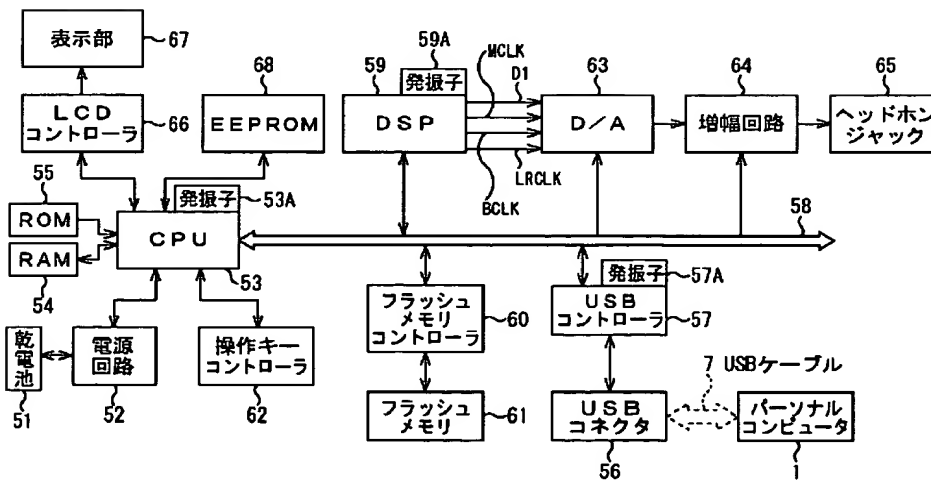
【図 2】



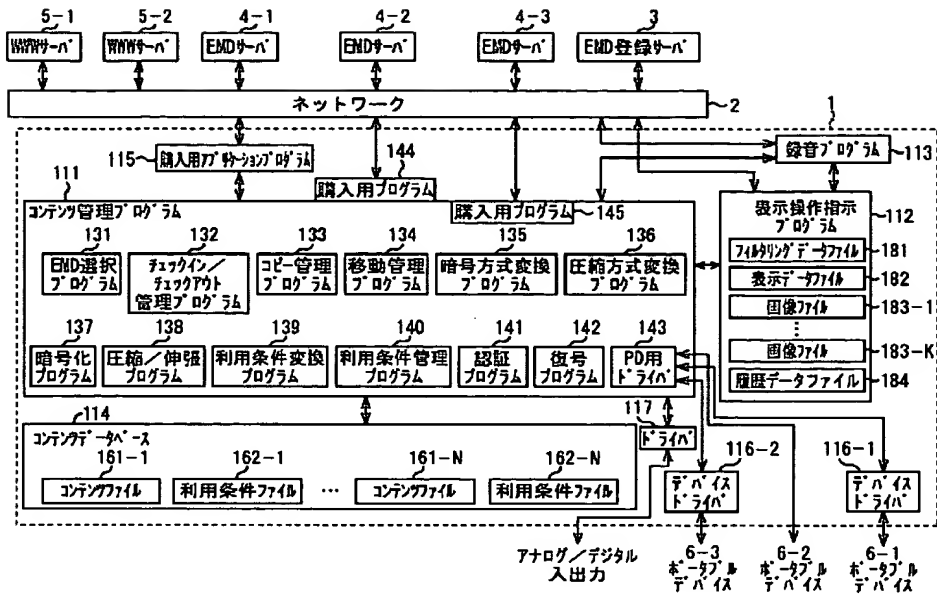
【図 6】



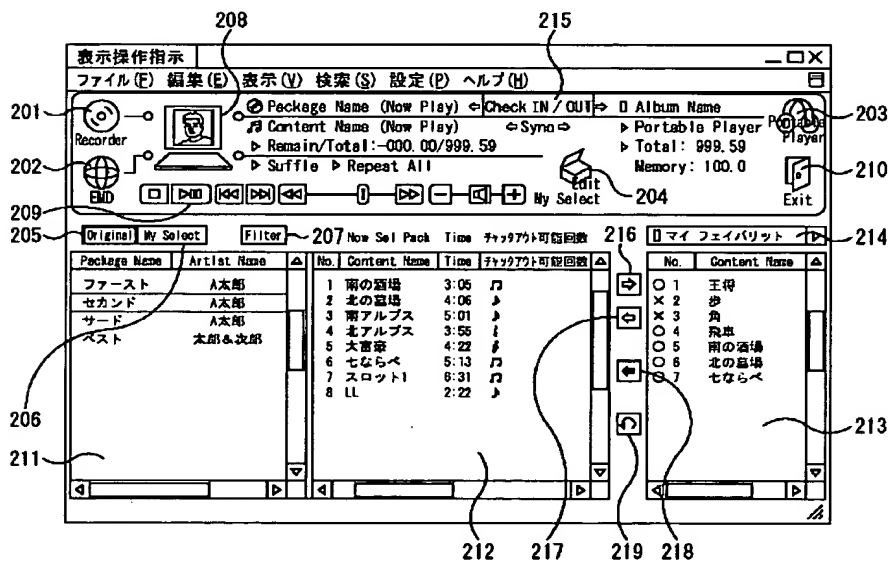
【図 3】



【図 4】



【図 5】



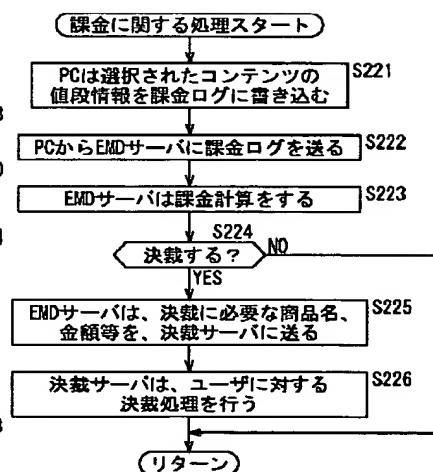
【図 9】

期限データベース

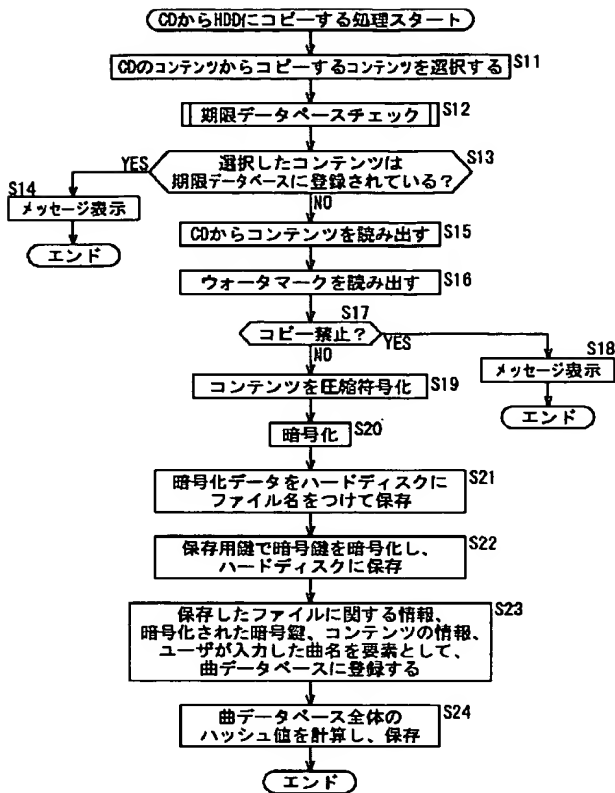
	アイテム1	アイテム2	アイテム3
ISRC	JP-Z90-98-12345	US-Z90-99-12346	JP-Z90-98-12347
コピー日時	1998.11.23.08:04	2004.03.06.16:09	2004.03.06.16.15

ハッシュ値 0xf3352e125934

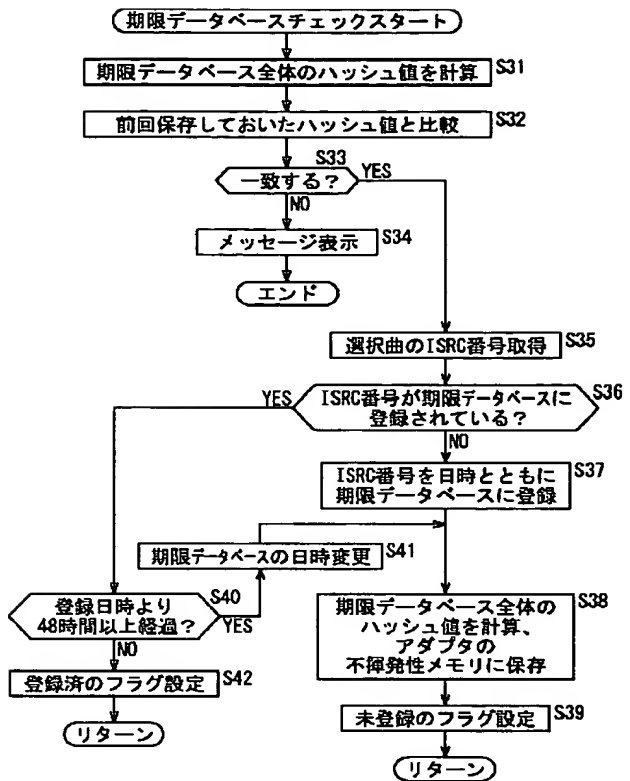
【図 24】



【図 7】



【図 8】



【図 11】

曲データベース

	アイテム1	アイテム2	アイテム3
ファイル名	xd000110.at2	px92341234.at2	aa0234287034.at2
暗号化された暗号鍵	0xabababababab	0x9898989898989898	0x123456789012
曲名	春の小川	運命	荒城の月
長さ	180	190	200
再生条件: 開始日時	-	2001.01.01.00:00	-
再生条件: 終了日時	1999.07.31.23:59	-	-
再生条件: 回数制限	-	20	-
再生回数カウンタ	-	12	-
再生時課金条件	-	-	¥5
コピー条件: 回数	2	0	0
コピー回数カウンタ	1	0	0
コピー条件: SCMS	0b01	0b10	0b00

ハッシュ値	0xf9951e566321
-------	----------------

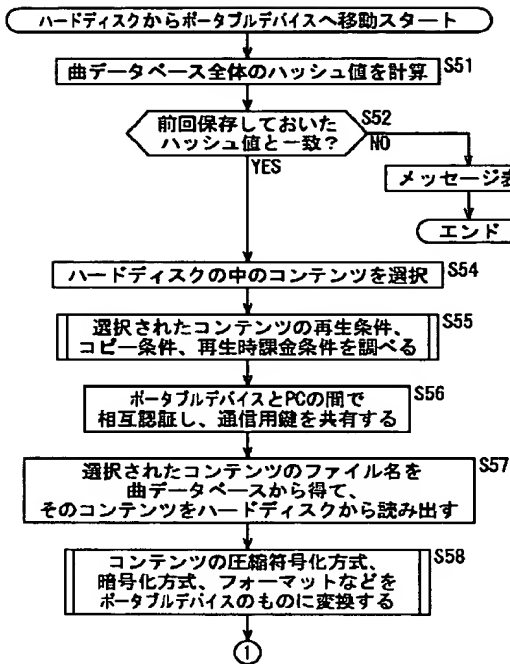
【図 16】

ポータブルデバイスが管理している再生条件

	アイテム1	アイテム2	アイテム3
コンテンツID	00001	00002	00003
再生開始日時	1999.07.31.23:59	1999.07.31.23:59	1999.07.31.23:59
再生終了日時	2001.01.01.00:00	2001.01.01.00:00	2001.01.01.00:00
再生回数	-	15	-

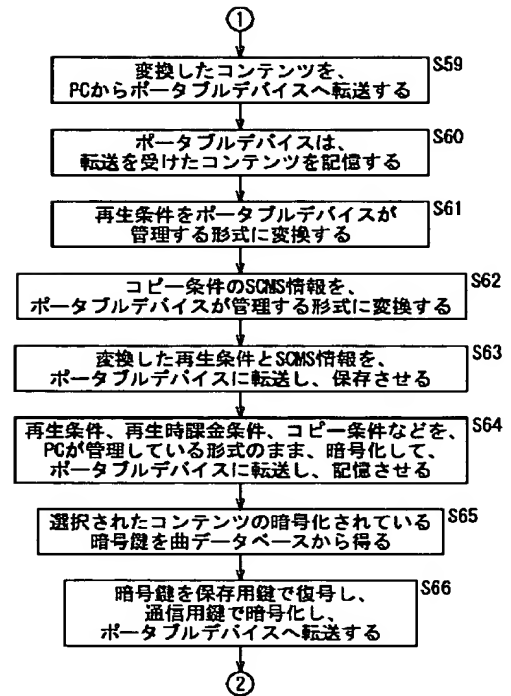
【図 1 2】

(12-1)



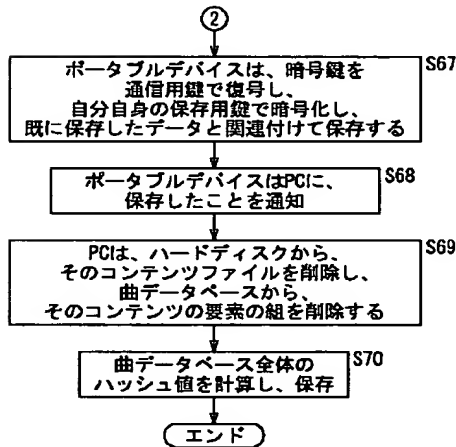
【図 1 3】

(12-2)

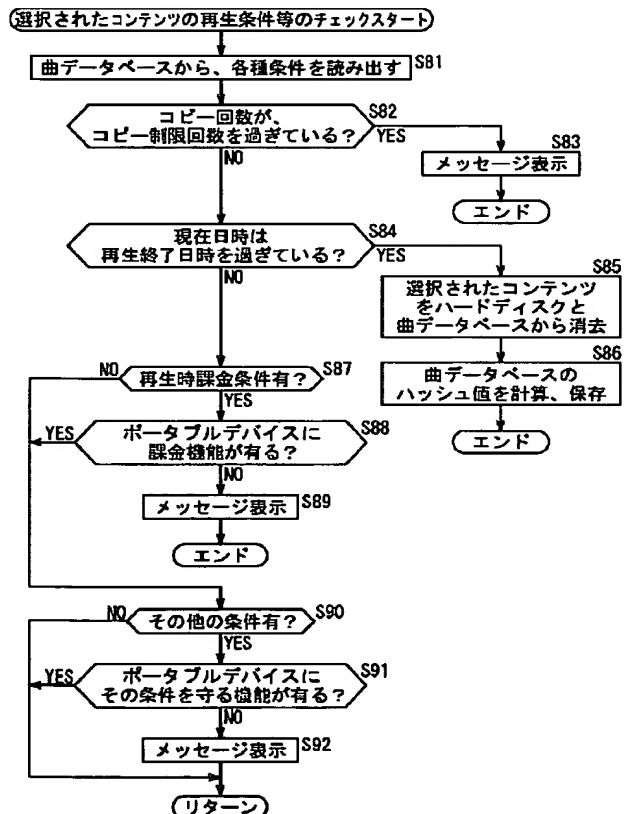


【図 1 4】

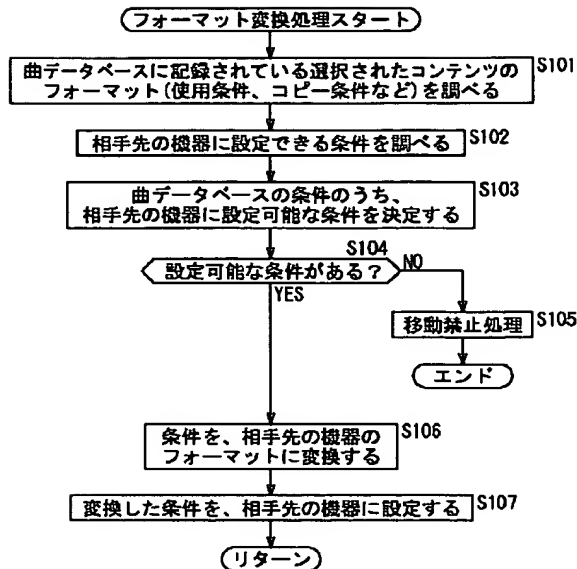
(12-3)



【図 1 5】

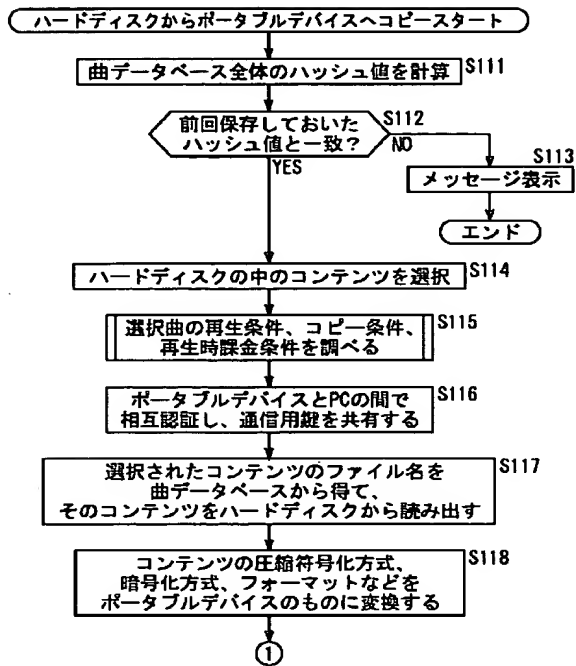


【図 17】



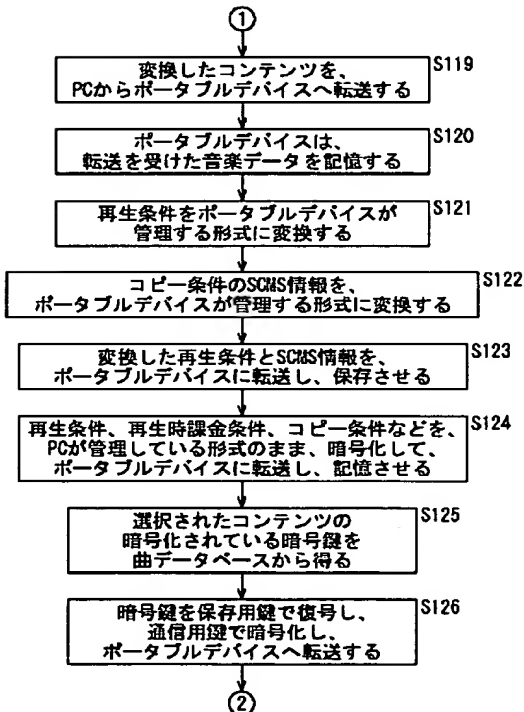
【図 18】

(18-1)



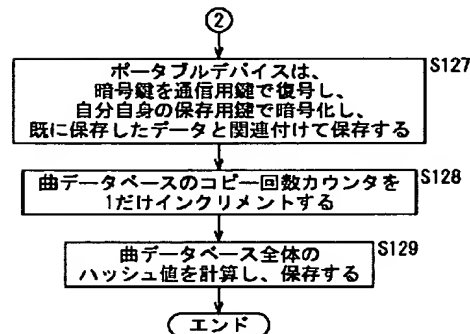
【図 19】

(18-2)

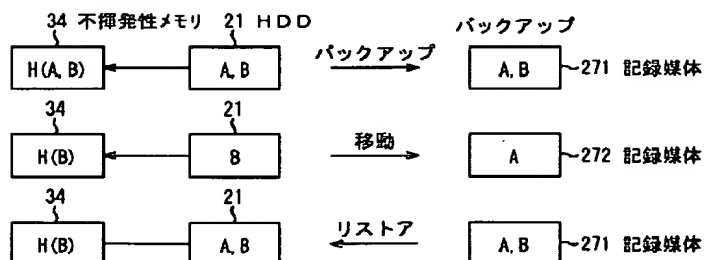


【図 20】

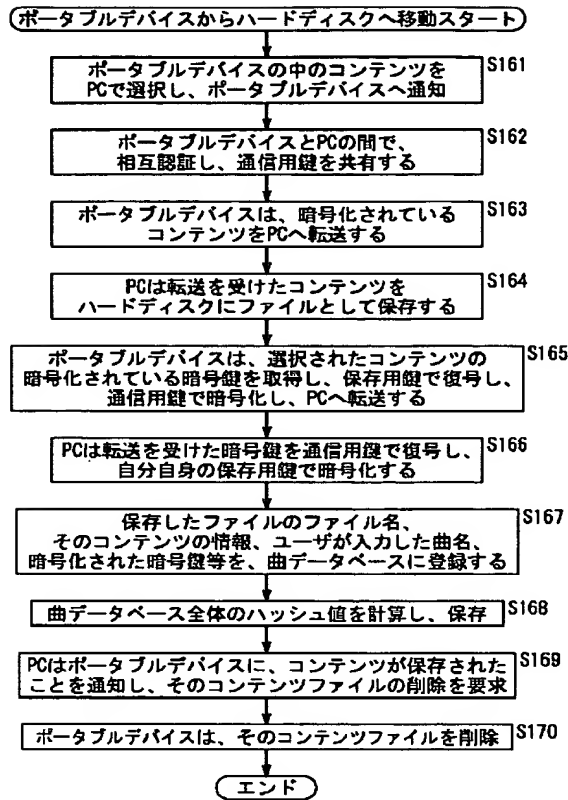
(18-3)



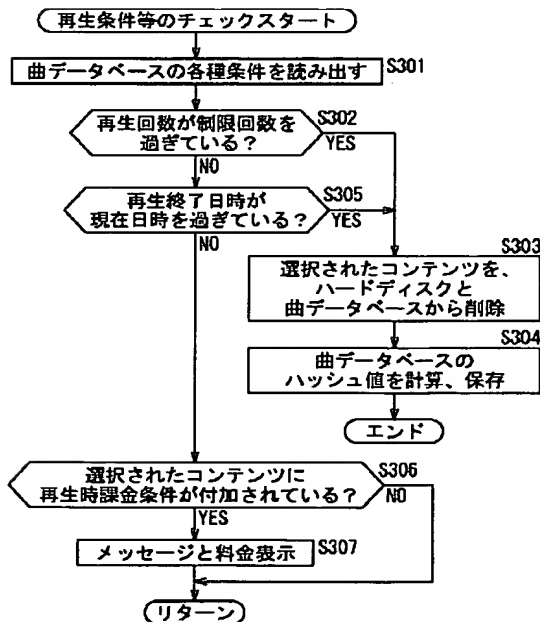
【図 33】



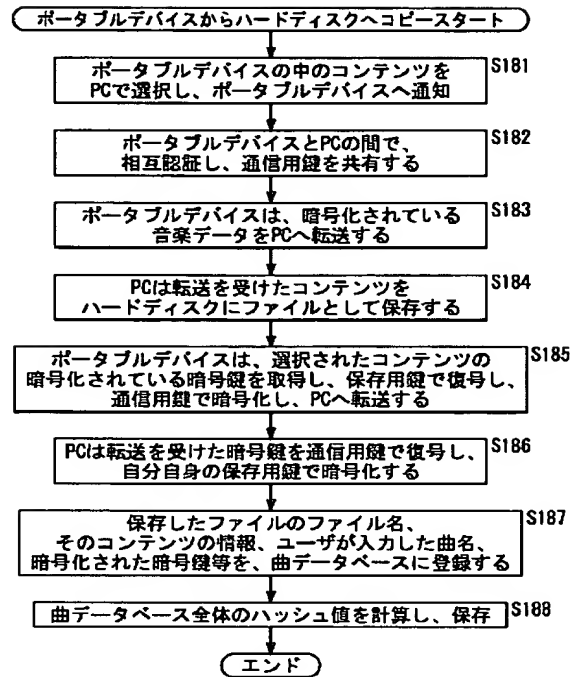
【図 2 1】



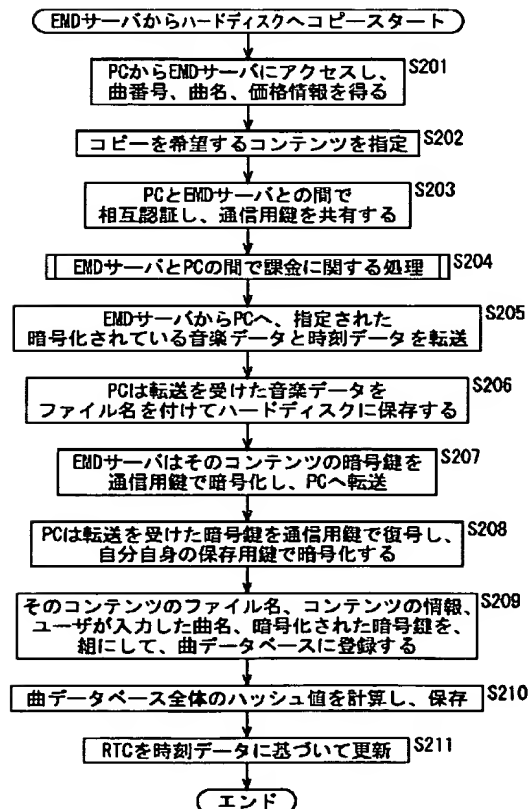
【図 3 0】



【図 2 2】



【図 2 3】



【図 25】

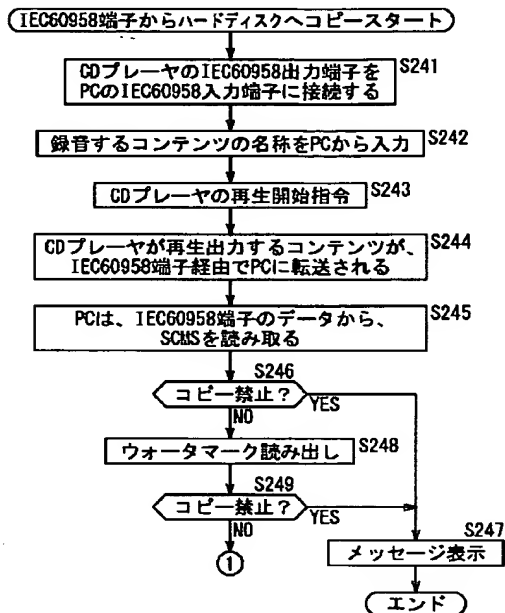
録金ログ

	アイテム1	アイテム2	アイテム3	
料金	50	50	60	

ハッシュ値	0xf8783e263517
-------	----------------

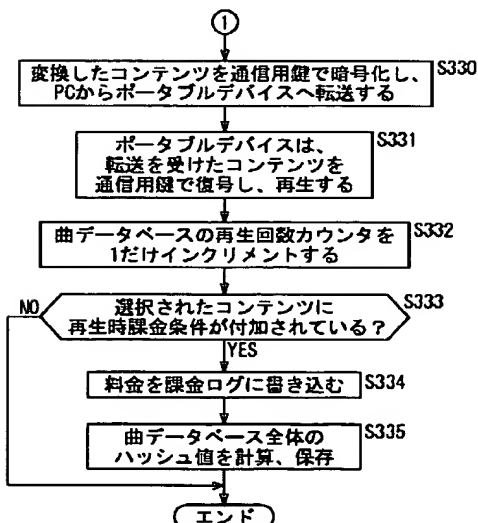
【図 26】

(26-1)



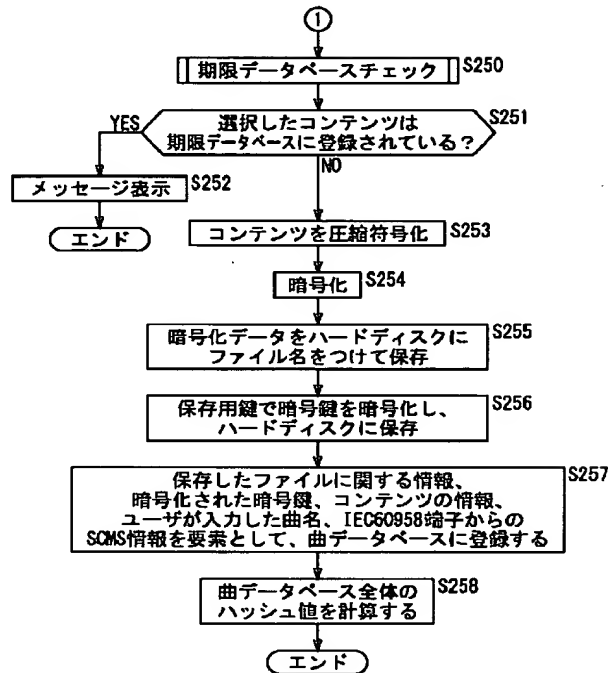
【図 32】

(31-2)

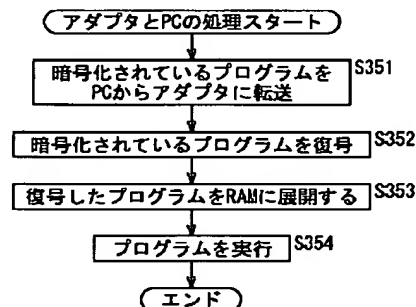


【図 27】

(26-2)

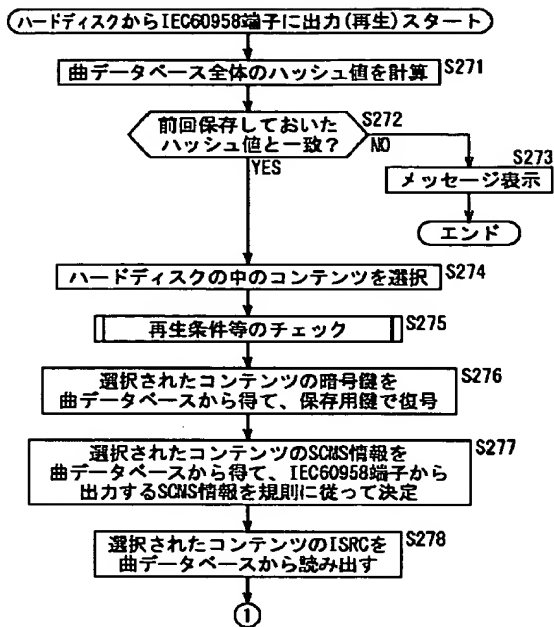


【図 34】



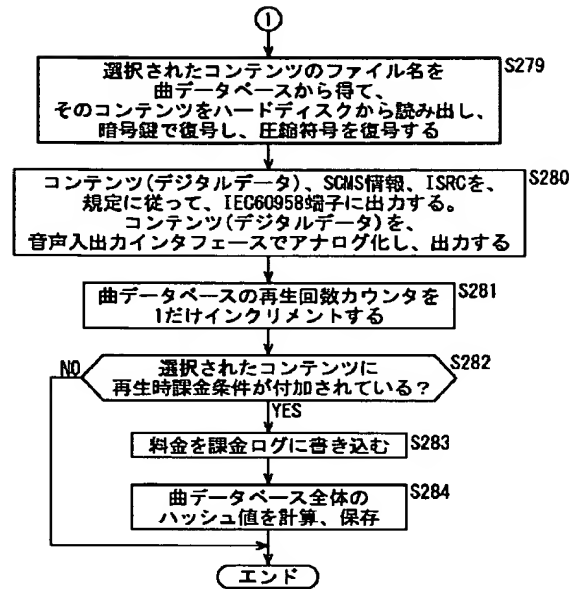
【図 28】

(28-1)



【図 29】

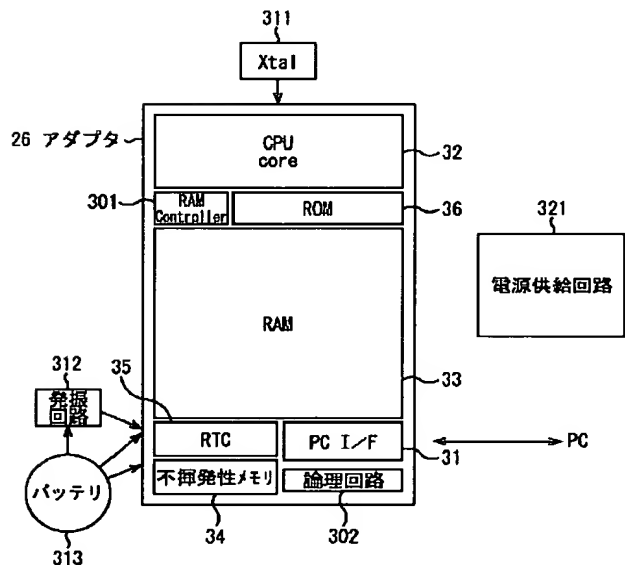
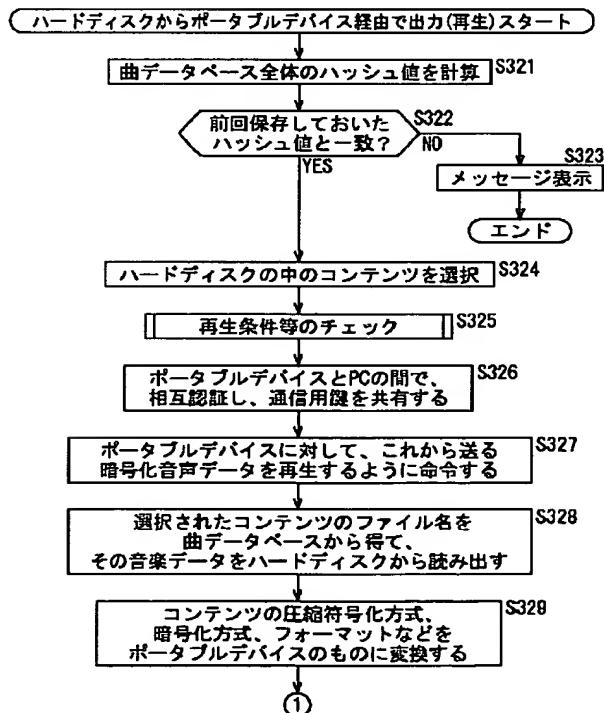
(28-2)



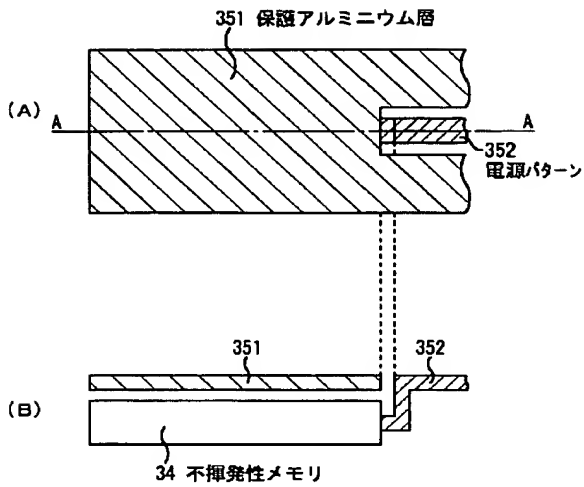
【図 35】

【図 31】

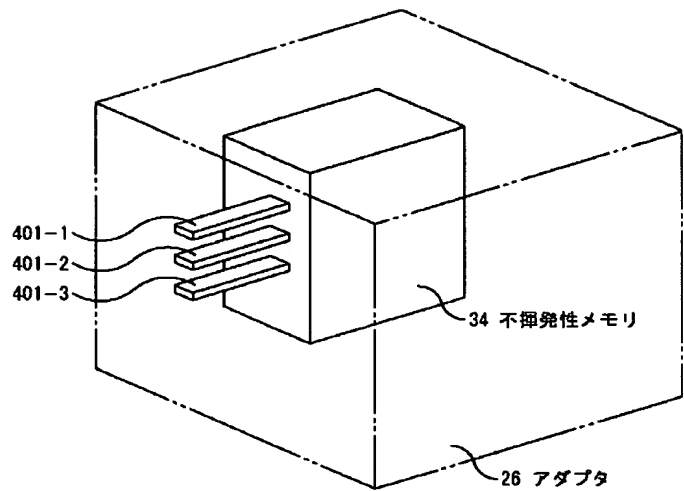
(31-1)



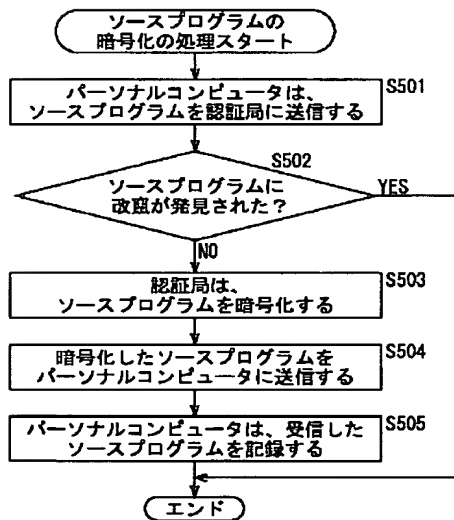
【図 36】



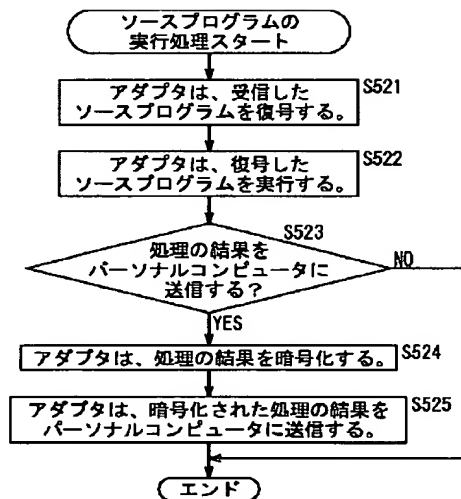
【図 37】



【図 42】

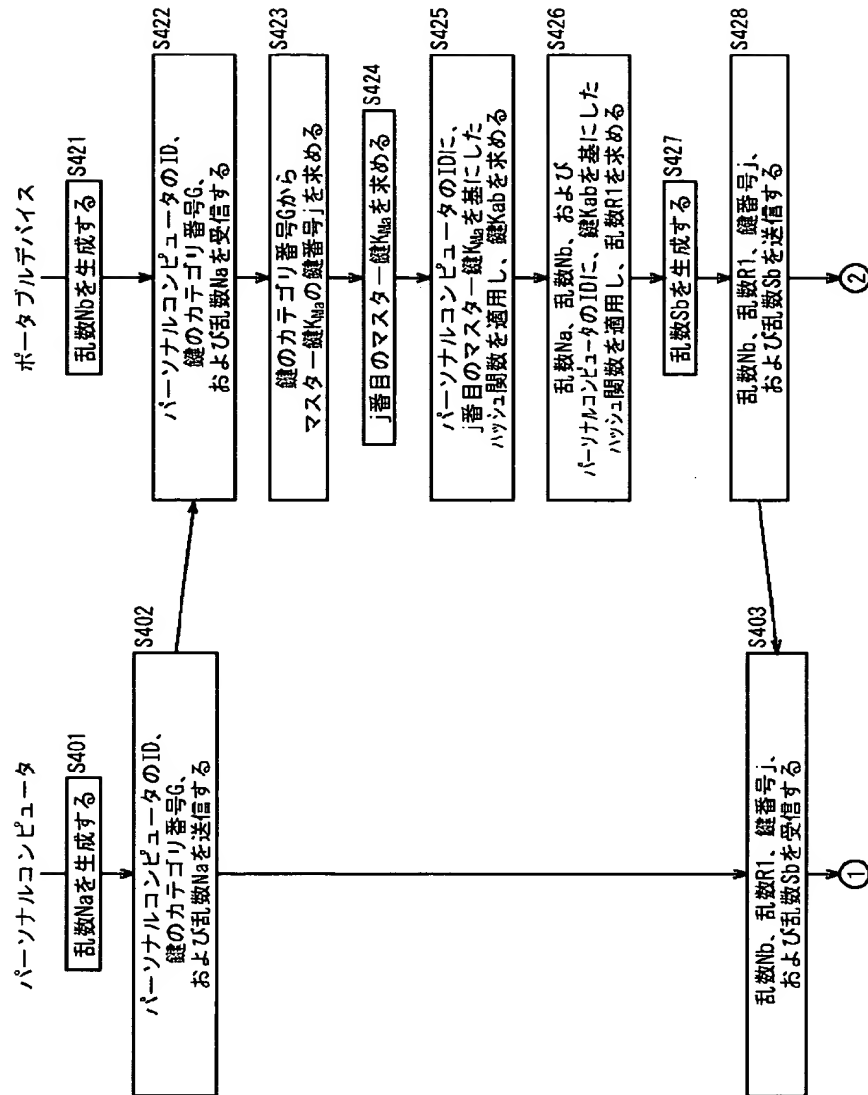


【図 43】



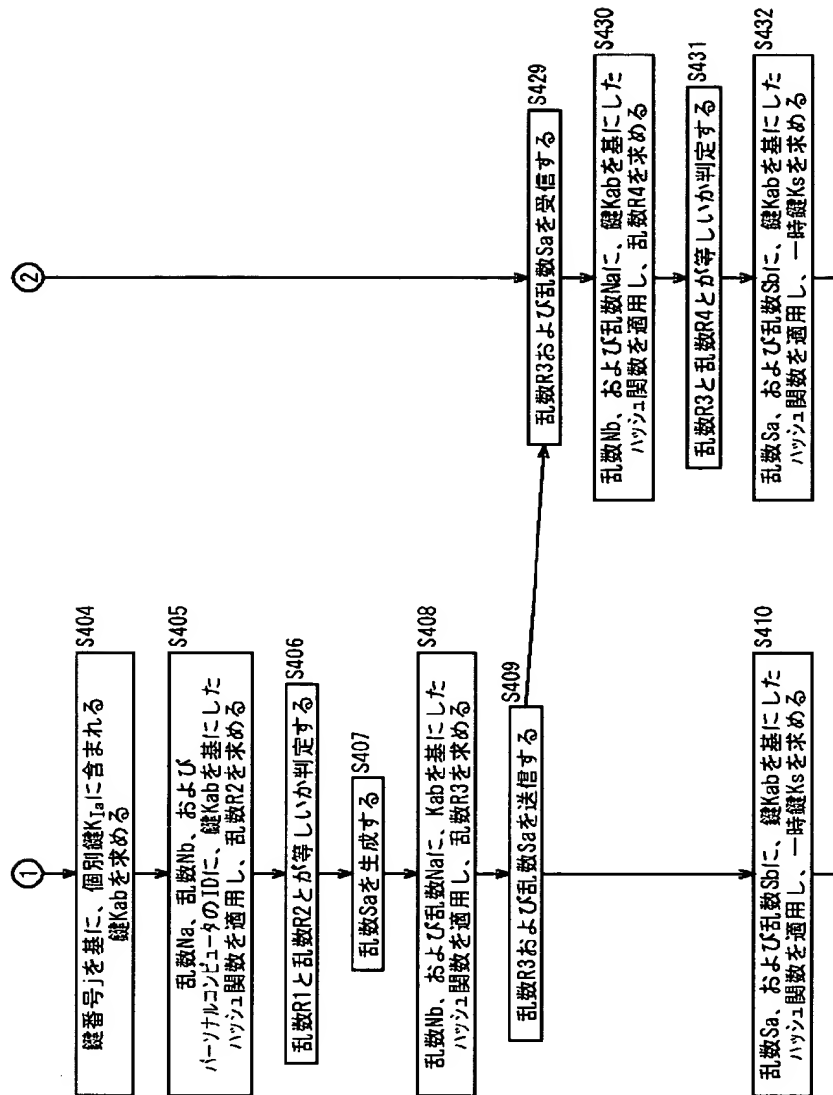
【図 38】

(38-1)



【図 39】

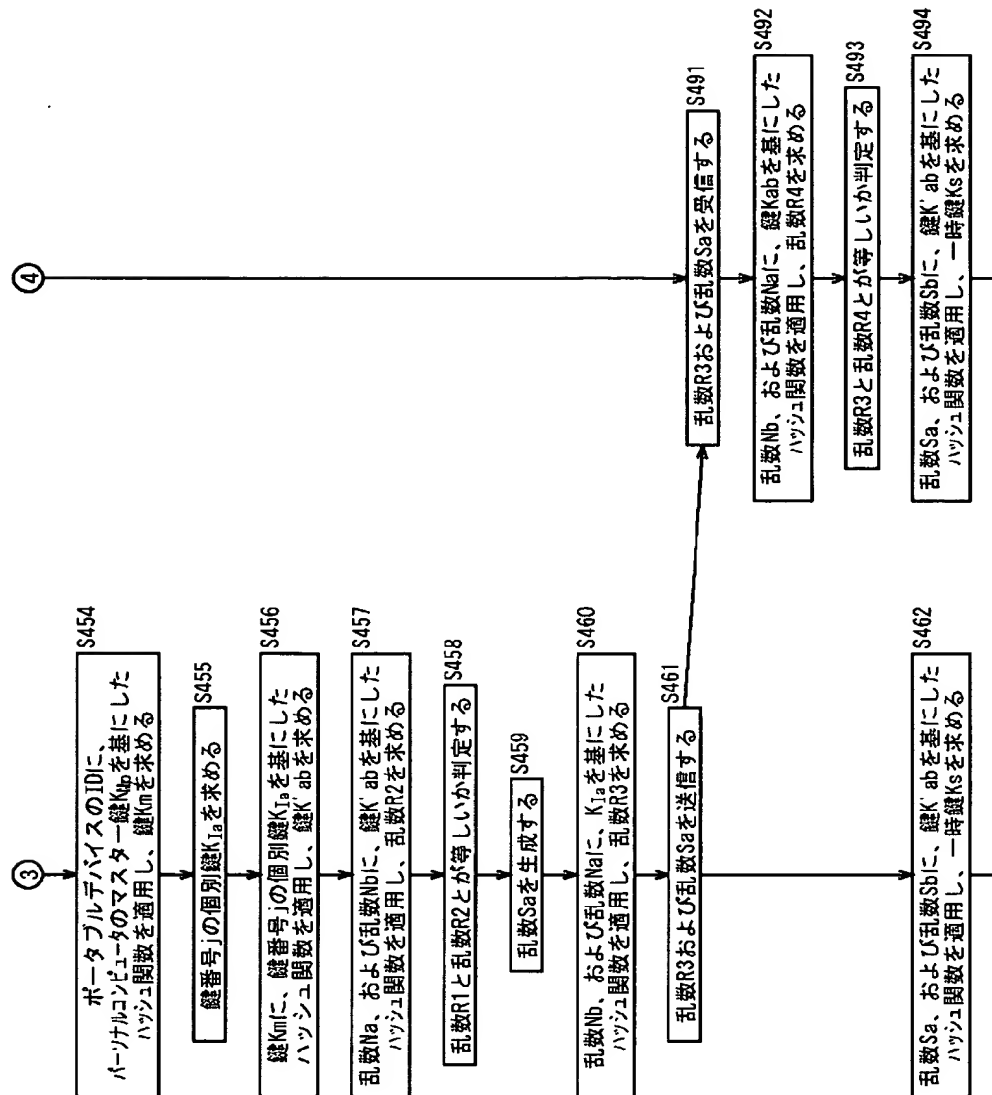
(38-2)



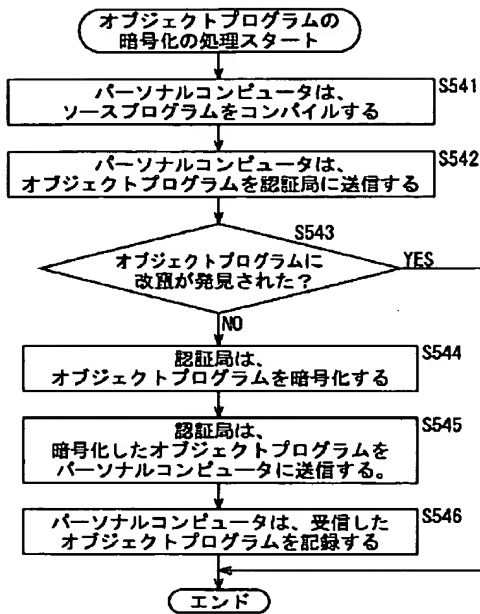


【図 41】

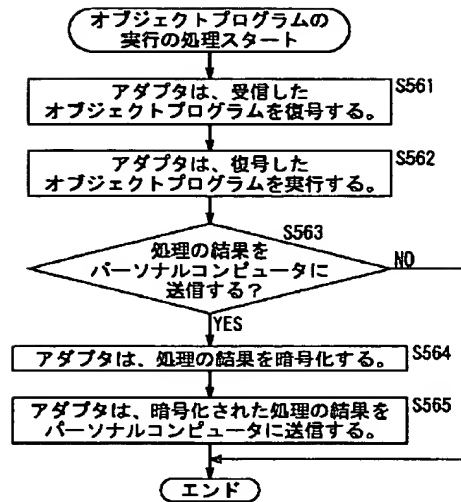
(40-2)



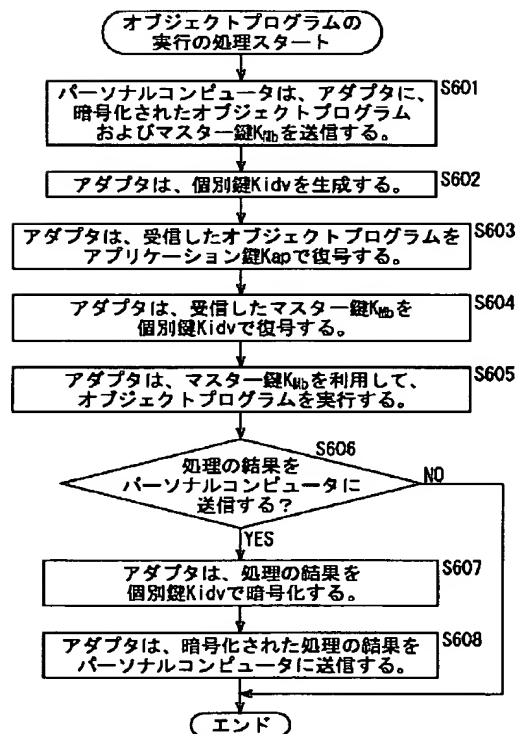
【図 4 4】



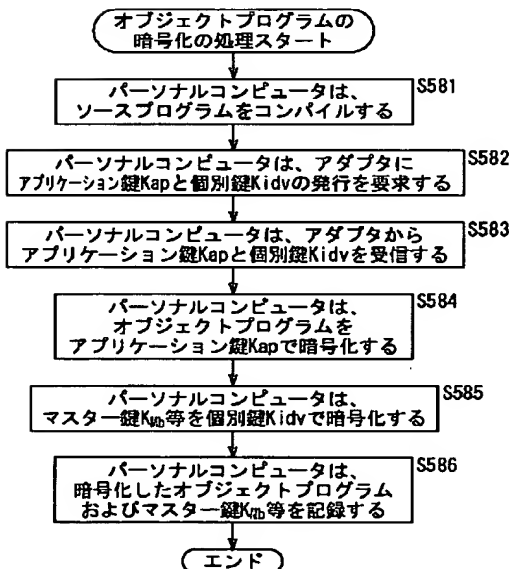
【図 4 5】



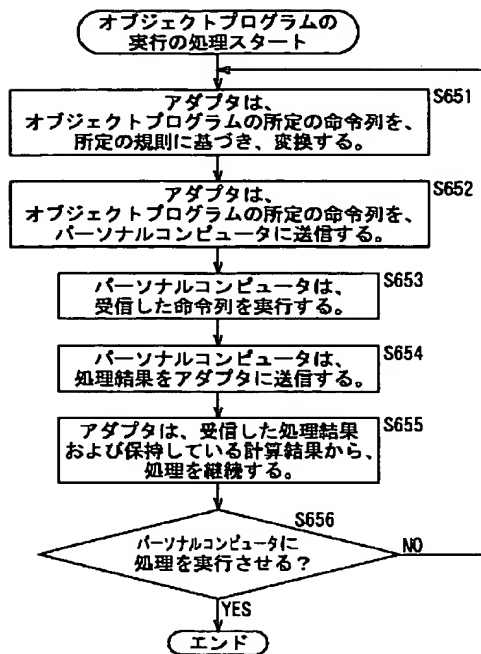
【図 4 7】



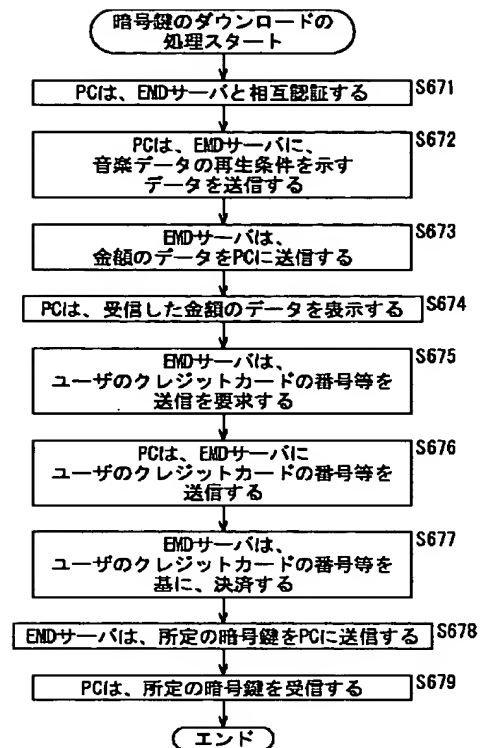
【図 4 6】



【図 48】



【図 49】



フロントページの続き

(72)発明者 田辺 充  
東京都品川区北品川 6 丁目 7 番35号 ソニ  
ー株式会社内

(72)発明者 江面 裕一  
東京都品川区北品川 6 丁目 7 番35号 ソニ  
ー株式会社内

(72)発明者 河原 博和  
東京都品川区北品川 6 丁目 7 番35号 ソニ  
ー株式会社内